

**Methods for emitting and receiving an image representing at least one object,
related electronic emission and reception devices and computer program products**

The present invention relates to a method for the transmission of an image
5 representing at least one object. The present invention further relates to a computer
program product suitable for implementing such a transmission method and to an electronic
device for transmitting an image representing at least one object.

The present invention further relates to a method of reception of such image. The
present invention further relates to a computer program product suitable for implementing
10 such a reception method and to an electronic device for receiving an image representing at
least one object.

The present invention relates more precisely to the field of encryption and decryption
of information contained in an image.

Public interest in the confidentiality of transmitted information has recently been
15 strongly reinforced, particularly with regard to the protection of personal data relating to
natural persons.

As an example, within the European union, the General Data Protection Regulation
(GDPR) illustrates this growing interest.

In particular, the regulation imposes confidentiality as the design standard for
20 personal data communication devices.

Thereby, during the transmission of information, it is henceforth recommended that
only users authorized to consult the transmitted information should be able to access said
information.

In the context of video surveillance, it is known how to transfer images via secure
25 communication channels. However, such communication is complex to implement.
Furthermore, such communication entails high costs because the means of communication
on secure channels require specific infrastructures.

In a variant, it is known how to apply total blurring to the images, to transmit same
in such state, and to communicate only to a chosen recipient, a key for deblurring the image
30 completely.

However, such on/off technique only ensures the confidentiality of personal data
when the recipient is authorized to consult the entire content of the images. Thereby, the
confidentiality of personal data is not optimal.

The aim of the present invention is to ensure, in a simple way, the confidentiality of
35 the personal data present on an image during the communication thereof.

To this end, the subject matter of the present invention relates to a method of transmission, from an electronic transmitter device and to at least one electronic receiver device, an image representing at least one object.

to the extent that the transmission method being implemented by the electronic transmission device and comprising a configuration phase includes the following step:

- sending to the or each electronic receiver device a respective individual secret key,

the method further comprising an encryption including the following steps:

- acquiring the image representing the at least one object, wherein one or a plurality of zones including certain pixels of the image are identified, each identified zone representing the or one of the objects,
- applying an obfuscation to the or each zone of the image, so as to form an image with obfuscated zone(s),
- generation of an encrypted message comprising values of the pixels of the zones in the image obtained, wherein said values are encrypted,
- transmission, to the or each electronic receiver device, of the image with obfuscated zone(s) and of the encrypted message for at least partial decryption, by each electronic receiver device in order to reconstruct a partially reconstructed image associated with the electronic receiver device,

wherein each individual secret key is calculated from a lookup table, the lookup table associating with each electronic receiver device a respective list of object(s) that the electronic receiver device is authorized to consult by decrypting the encrypted message, using said individual secret key.

With the transmission method according to the invention, it is possible to transmit an image that protects the personal data, while being partially decryptable for a user authorized to consult part of the content thereof.

Such effect is obtained in particular by means of the obfuscation of the identified zone(s), as well as by the individual secret key suitable for the decryption of only certain pixel values, i.e. of certain zone(s).

According to other particular embodiments, the transmission method comprises one or a plurality of the following features, captured individually or according to all technically possible combinations:

- the acquiring step includes the sub-steps of:
 - o image acquisition, and

- identification in the acquired image of zone(s) representing the or each object on the basis of an identification model,

the identification step is preferentially implemented by an identification model comprising more preferentially a neural network;

- the configuration phase further includes the following steps prior to the sending step:

- acquisition of the lookup table,
- determination of a master public key and of a master secret key,
- calculation, for each electronic receiver device, of the respective individual secret key from the master secret key and the list of object(s) associated with that electronic receiver device in the lookup table,

during the generation step, the pixel values are encrypted on the basis of the master public key,

the master public key and the individual secret keys preferentially being distinct, the individual secret keys preferentially still being distinct from each other;

- the generation step comprises the following sub-steps:
 - storage, in a message, of pixel values corresponding to the zone(s) identified in the image,
 - application of an encryption algorithm to the pixel values of the message from the master public key, so as to form the encrypted message,
- the encryption algorithm being preferentially chosen from the group consisting of:
- the BSW07 algorithm,
 - the CPW08 algorithm, and
 - the AC17 algorithm; and

- the image obtained comes from a camera chosen from a predefined list of cameras, the lookup table associating, for each electronic receiver device, for each object, one or a plurality of cameras suitable for taking images for which the electronic receiver device is authorized to consult said object,
- the or each individual secret key further depending on the camera or cameras associated with the corresponding electronic receiver device in the lookup table.

The invention further relates to a computer program product comprising software instructions which, when executed by a computer, implement a reception method as defined hereinabove.

A further subject matter of the present invention is an electronic device for transmitting, to at least one electronic receiver device, an image representing at least one

object among a predefined list of object(s), the electronic transmitter device comprising a configuration unit comprising:

- a sending module configured to send to the or each electronic receiver device, a respective individual secret key,

5 the electronic transmitter device further comprising an encryption unit comprising:

- an acquisition module configured to acquire the image representing the at least one object, wherein one or a plurality of zones including certain pixels of the image are identified, each identified zone representing the or one of the objects,
- an application module configured to apply a masking to the or each zone of the
- 10 image, so as to form an image with obfuscated zone(s),
- a generator module configured to generate an encrypted message comprising pixel values of the zones in the resulting image, wherein the pixel values are encrypted,

- a transmission module configured to transmit, to each electronic receiver device,
- 15 the image with obfuscated zone(s) and the encrypted message for at least partial decryption, by each electronic receiver device, so as to reconstruct a partially reconstructed image associated with the respective electronic receiver device,

wherein each individual secret key is calculated from a lookup table, the lookup table associating with each electronic receiver device a respective list of object(s) that the

20 the electronic receiver device is authorized to consult by decrypting the encrypted message, on the basis of said individual secret key.

A further subject matter of the present invention is a method for receiving, by an electronic receiver device and from an electronic transmitter device, an image with at least one obfuscated zone suitable for representing an object from a predefined list of object(s),

25 the method being implemented by an electronic receiver device and comprising the following steps:

- reception of the image with obfuscated zone(s), an encrypted message comprising encrypted pixel values, and an individual secret key associated with the electronic receiver device,

30 the individual secret key being suitable for decrypting only the encrypted pixel values corresponding to one or a plurality of zones of the image with obfuscated zone(s) representing objects which the electronic receiver device is authorized to consult,

- decryption, on the basis of a decryption algorithm and the received individual
- 35 secret key, of the encrypted pixel values of the encrypted message, so as to acquire a partially decrypted message, and

- reconstruction of a partially reconstructed image by replacing the obfuscated zone(s) of the image with obfuscated zone(s) with pixels the values of which are comprised in the partially decrypted message,

at least one zone of the partially reconstructed image representing an object that the electronic receiver device is authorized to consult.

With the reception method according to the invention, it is possible to decrypt only a part of an image for which only certain objects are authorized to be consulted.

Such effect is obtained in particular by the individual secret key, which only allows decrypt part of the encrypted message to be encrypted. Thereby, the partially reconstructed image preserves the confidentiality of the objects that the receiver device is not authorized to consult.

The invention further relates to a computer program product including software instructions which, when executed by a computer, implement a reception method as defined hereinabove.

A further subject matter of the present invention is an electronic receiver device for receiving, from an electronic transmission device, an image with at least one obfuscated zone suitable for representing an object, the electronic receiver device comprising:

- a reception module configured to receive the image with obfuscated zone(s), an encrypted message comprising encrypted pixel values, and an individual secret key (I_s) associated with said electronic receiver device, the individual secret key being able to decrypt only the encrypted pixel values corresponding to one or a plurality of zones of the image with obfuscated zone(s) representing objects which the electronic receiver device is authorized to consult,
- a decryption module configured to decrypt, from a decryption algorithm and the received individual secret key (I_s), the encrypted pixel values of the encrypted message in order to acquire a partially decrypted message, and
- a configured reconstruction module reconstructing a partially reconstructed image by replacing the obfuscated zone(s) of the image with obfuscated zone(s) with pixels the values of which are comprised in the partially decrypted message,

at least one zone of the partially reconstructed image representing an object that the electronic receiver device is authorized to consult.

A further subject matter of the present invention is an electronic communication system comprising an electronic transmitter device and at least one electronic receiver device,

wherein the transmitter electronic device is defined hereinabove and each electronic receiver device is also defined hereinabove.

The communication system makes it possible to improve, in a simple way, the confidentiality of personal data.

The features and advantages of the invention will appear upon reading the following description, given only as an example, but not limited to, and making reference to the enclosed drawings, wherein:

- Figure 1 is a schematic representation of a communication system according to the invention comprising an electronic transmitter device and at least one electronic receiver device according to the invention;
- Figure 2 is an example of an image acquired by the electronic transmitter device shown in Figure 1;
- Figure 3 is an example of an image with obfuscated zone(s) transmitted by the electronic transmitter device shown in Figure 1 to the electronic receiver device(s) shown in Figure 1;
- Figure 4 is an example of a partially reconstructed image obtained by the or one of the electronic receiver devices shown in Figure 1;
- Figure 5 is a flowchart of a transmission method according to the invention, the method being implemented by the electronic transmitter device shown in Figure 1; and
- Figure 6 is a flowchart of a reception method according to the invention, the method being implemented by the electronic receiver device shown in Figure 1.

With reference to Figure 1, an electronic communication system 10 is described. The electronic communication system 10 is suitable for being connected to a camera 15.

The communication system 10 comprises an electronic transmitter device 20 and at least one electronic receiver device 25. In the example shown in Figure 1, the communication system 10 comprises a plurality of receiver devices 25.

The camera 15 is e.g. a video surveillance camera in a street of a city. The camera 15 is suitable for capturing images 37 of an environment. On the images captured 37 by the camera 15, there are visible e.g. a plurality of objects of interest, also called objects. The objects of interest include e.g. outlines of passers-by in the street, faces of the passers-by, and vehicles.

Thereby, each image captured 37 by the camera 15 represents at least one of said objects.

The camera 15 is e.g. connected to the transmitter device 20 and apt to send the captured images 37 thereto.

The transmitter device 20 comprises a configuration unit 30 and an encryption unit 35.

The configuration unit 30 comprises a module 40 for sending individual secret key(s) I_s to each receiver device 25. Preferentially, the configuration unit 30 further comprises a module 42 for acquiring a lookup table, a module 44 for determining a master public key M_p and a master secret key M_s , and a module 46 for calculating the individual secret key(s) I_s .

The encryption unit 35 comprises a module 50 for acquiring at least one respective image 37 from the camera 15, a module 52 for applying an obfuscation to parts of the image which will be discussed in detail hereinafter, a module 54 for generating an encrypted message and a transmitter module 56 for transmitting to each receiver device 25, elements coming from the application module 52 and the generator module 54.

Each receiver device 25 comprises a reception module 60, a module 62 for decrypting the encrypted message and a module 64 for reconstructing an image.

Each receiver device 25 is associated with a user. In the example shown in Figure 1, the communication system 10 comprises a first 25A, a second 25B and a third 25C receiver devices. The first receiver device 25A is e.g. associated with a security guard monitoring an entrance to a car park. The second receiver device 25B is e.g. associated with a police department. The third receiver device 25 is e.g. associated with a committing magistrate. In the present example, the security guard is only allowed to consult the "vehicle" objects in the images 37. The police department is only allowed to consult the "outline" objects of the images 37. Finally, the committing magistrate is authorized to consult all objects, i.e. the vehicles, the outlines and the faces, in the image 37.

Preferentially, each receiver device 25 further comprises a respective display screen 67.

The sending module 40 is configured to send, to each receiver device 25, the individual secret key I_s specific to same. To this end, the sending module 40 is configured to send the key I_s via a secure channel, e.g. a TLS, such as an HTTPS channel that is encrypted and authenticated.

Each individual secret key I_s is e.g. stored in the configuration unit 30. Each individual secret key I_s is a respective one of a receiver device 25. In the case where the communication system 10 comprises several receiver devices 25, the individual secret keys I_s are distinct from one another.

Each individual secret key I_s is suitable for a decryption of the encrypted message in order to reveal the objects that the user of the receiver device 25 to which said key I_s sent, is authorized to consult.

In the example described hereinabove, the sending module 40 is configured to send a first I_{s1} , a second I_{s2} , and a third I_{s3} individual secret keys.

More particularly, the sending module 40 is configured to send:

- to the first receiver device 25A, the first individual secret key I_{s1} , which is suitable for decrypting objects representing vehicles,
- to the second receiver device 25B, the second individual secret key I_{s2} , which is suitable for decrypting objects representing silhouettes, and
- to the third receiver device 25C, a third individual secret key I_{s3} , which is suitable for decrypting all the objects, i.e. vehicles, silhouettes and faces.

Optionally, the acquisition module 42 is configured to acquire the lookup table. The lookup table associates, with each receiver device 25, a respective list of object(s) that said receiver device 25 is authorized to consult by decrypting the encrypted message using the respective individual secret key I_s . In the aforementioned example, the lookup table associates:

- the "vehicle" object with the first receiver device 25A;
- the object "outline" with the second receiver device 25B; and
- the objects "vehicle", "outline" and "face" with the third receiver device 25C.

The determination module 44 is configured to determine the master public key M_p and the master secret key M_s . In a way known per se, the master public key M_p is configured to encrypt data that can be decrypted by means of the master secret key M_s .

The master public key M_p and the master secret key M_s are preferentially distinct from each other. Thereby, the master public key M_p can be consulted by anyone wishing to encrypt data. The master secret key M_s is kept secret, i.e. confidential, by the configuration unit 30. The master secret key M_s is preferentially not communicated to any other electronic device.

The master public key M_p and master secret key M_s are e.g. determined randomly.

The calculation module 46 is configured to calculate, for each electronic receiver device 25, the respective individual secret key I_s , e.g. on the basis of the master secret key M_s and of the list of object(s) associated with the electronic receiver device 25 in the lookup table.

The calculation module 46 is configured e.g. to apply a key generation function of an attribute encryption algorithm, also known as the Attribute-Based Encryption (ABE) algorithm, wherein each attribute is an object. Thereby, the calculation module 46 is

configured to calculate an individual secret key I_s for each receiver device 25 from the objects that said receiver device 25 is authorized to consult in the lookup table.

The calculation of each individual secret key I_s depends on the type of ABE algorithm used. Preferentially, algorithm ABE is chosen from the following algorithms:

- BSW07 described in the article Ciphertext-Policy Attribute-Based Encryption by Bethencourt et al,
- CPW08 described in Ciphertext-Policy Attribute-Based Encryption: An Expressive, Efficient, and Provably Secure Realization by Waters et al, and
- AC17 described in FAME article: Fast Attribute-based Message Encryption by Agrawal and al.

Thereby, the calculation module 46 is configured to calculate the individual secret key(s) I_s , such that each individual secret key I_s can be used only for decrypting the object(s) associated with the corresponding receiver device 25 in the lookup table.

"Decrypting an object" means decrypting encrypted pixel values associated with the object, as will be described hereinafter.

The acquisition module 50 is configured to acquire the image 37 representing at least one object, wherein one or a plurality of zones 70 are identified as representing the object or one of the objects. Each zone 70 includes certain pixels of the image 37.

The expression "certain pixels of the image" is understood in the sense that only a part of the pixels of the image is comprised in each zone 70.

In a way known per se, each image is composed of a plurality of elements, e.g. pixels. Each pixel is defined by the spatial position thereof in the image and by an n-tuple of values. Each value is called a channel or a spectral band.

For example, the image is a so-called RGB image, wherein the n-tuple of values is a triplet of values corresponding to the colors red, green and blue. Each value of the triplet of values is comprised e.g. between 0 and 255. The higher the value associated with a color, the more the pixel has a dark shade of said color. In a variant, when the image 37 is in grayscale, a single value corresponding to a gray level is then associated with each pixel. In such case, a maximum value (e.g. 255) corresponds to a white pixel, while a minimum value (e.g. equal to 0) corresponds to a black pixel, or vice versa.

According to one embodiment, the acquisition module 50 is configured to acquire, from the camera 15, the image 37 captured by said camera 15.

Figure 2 shows such an image 37. In particular, it can be seen in Figure 2 that five vehicles, five outlines and two faces are identified.

The acquisition module 50 is further configured to identify, in the acquired image 37, the zone or zones 70 representing the or each object, on the basis of an identification

model. The identification model comprises e.g. a neural network, preferentially a neural network trained to detect the zone or zones 70 corresponding to each type of object in the image 37 and to classify each detected zone among a plurality of classes each corresponding to an object. Each of the zones is referred to hereinafter as the identified zone 70. In a way known per se, the neural network comprises a plurality of artificial neurons organized in layers. The neural network then consists of an input or one or a plurality of hidden or intermediate layers, and an output layer. The neurons of two successive layers are connected to each other by a link comprising an adjustable weight, also called synaptic weight.

Preferentially, the acquisition module 50 is configured to detect a portion of the acquired image 37 occupied by each object and to assign same a belonging to a specific class among the objects of the lookup table.

Preferentially, the detection comprises the definition, by the trained neural network, of a rectangular encompassing box around the object. Each encompassing box then forms a respective identified zone 70.

According to a variant (not shown), the acquisition module 50 is configured to segment the object more finely in the acquired image 37 by making masks on the objects, i.e. to assign a name to each pixel of the image. Thereby, each identified zone 70 is formed by all the pixels of the image comprising the same name. It should be then understood that the shape of the zones identified 70 according to such variant is not necessarily rectangular.

The application module 52 is configured to apply an obfuscation to the or each identified zone 70, in order to form an image with obfuscated zone(s) 75.

“Obfuscation” means a modification of the value(s) of a set of pixels in order to camouflage an object represented in the pixels.

According to an example shown in Figure 3, the obfuscation is a blurring. The application module 52 is configured e.g. to divide each identified zone 70 into group(s) of a plurality of pixels and to calculate, for each group, an average value of the values of the pixels of the group. The application module 52 is configured to then replace each pixel of each group with a pixel having the calculated average value. If each pixel comprises a triplet of values, said mean value is the mean of each value of the triplet. Alternatively, the blurring comprises applying a blurring filter to the identified zones 70, such as a Gaussian filter.

In a variant, the obfuscation is a masking comprising the replacement of each identified zone 70 by a shape the pixels of which have a predefined color, preferentially a monochrome shape, consisting e.g. of black pixels.

The application module 52 is configured to acquire an obfuscated zone image 75 wherein the or each identified zone 70 is modified by the application of the obfuscation and

wherein portions of the image not corresponding to an identified zone 70 are not affected by the obfuscation.

The generator module 54 is configured to generate an encrypted message, also called a secure message, comprising the values of the pixels of each identified zone 70 in the image acquired 37 by the acquisition module 50. The pixel values present in the encrypted message are encrypted. For this purpose, the generator module 54 is configured e.g. to store, in a message, the values of the pixels corresponding to the identified zone(s) 70 in the obtained image 37. The message is e.g. a database.

More particularly, the generator module 54 is configured so that the message comprises, for each identified zone 70, a plurality of data fields. For each identified zone 70, a first data field includes the position of said zone 70 in the image 37. For each identified zone 70, a second data field includes the values of the pixels of said zone 70. The first and second data fields are e.g. ordered so that the message comprises, for each identified zone 70, the first data field relating to the identified zone 70, then the second data field relating to said identified zone 70.

Preferentially, the message further comprises, for each identified zone 70, a third data field comprising a first character string indicating the object represented in said zone 70. For example, for each identified zone 70, the third data field is located, in the message, between the first and second data fields.

In the example described hereinabove, the message comprises the first data field including the position of a zone 70 in the image 37, then the third data field including a first respective character string "face", then the second data field including the pixel values ordered in a predefined way, corresponding to the zone 70 representing a face in image 37.

The generator module 54 is further configured to apply an encryption algorithm to the values of the pixels of the message, on the basis of the master public key M_p , so as to form the encrypted message. The values of pixels encrypted in the encrypted message, associated with each identified zone 70, form "an encrypted part". Thereby, it should be understood that the encrypted or secure message comprises an encrypted part for each identified zone 70.

More particularly, the generator module 54 is configured e.g. to apply the encryption algorithm only to the content of the second data field in the message. In other words, the contents of the first data field, and optionally the contents of the third data field, are not encrypted by the encryption algorithm. More specifically, the generator module 54 is configured e.g. to encrypt the values of the pixels in the following way.

The determination module 54 is configured to apply an encryption algorithm to each set of pixel values depending on the master public key M_p and, if appropriate, on an

encryption policy. The encryption algorithm depends on the applied ABE algorithm such as the BSW07, CPW08, or AC17 described hereinabove.

The encryption policy associates with each identified zone 70 a logical relation depending on the object or the objects represented in the identified zone 70, and e.g. on context element(s), on the basis of the lookup table.

Each logical relation can be typically formulated, according to Boolean algebra, by a logical equation including at least one operand and, if appropriate, one or a plurality of operators. Each operand is an object of the lookup table and/or a context element. Each operator is preferentially chosen from the following operators: "AND", and "OR".

Thereby, e.g., in the case of superposition of two objects in the image 37, an identified zone 70 partially encompasses another identified zone, the policy includes a logical relationship associated with the partially encompassed zone of the type "first object AND second object" or of the type "first object OR second object";

When the logical relationship is of the type "first object AND second object", the pixels of said partially encompassed zone 70 are encrypted so that only a receiver device 25 having an individual secret key corresponding to the first object and to the second object can decrypt the pixels.

When the logical relation is of the type "first object OR second object", the pixels of said partially encompasses zone are encrypted so that only a receiver device 25 having an individual secret key corresponding to the first object or to the second object can decrypt the pixels.

It should be understood that the third data field comprises the logical relation associated with the corresponding identified zone 70 in the encryption policy.

The transmission module 56 is configured to transmit, to each receiver device 25, the image with obfuscated zone(s) 75 and the encrypted message. Preferentially, the encrypted message is included in metadata of the transmitter image with obfuscated zone(s) 75.

It should be then understood that a third party intercepting the image with obfuscated zone(s) 75 and the encrypted message sent by the transmission module 56 is not able to consult the objects of the identified zones 70 in the acquired image 37, i.e. the objects the pixel values of which have been encrypted in the encrypted message.

Furthermore, the image with obfuscated zone(s) 75 and the encrypted message are transmitted e.g. over an unsecured channel, without any risk to the confidentiality of personal data being incurred.

Relating to each receiver device 25, the reception module 60 thereof is configured to receive, from the transmission device 20, and more particularly from the transmission

module 56 of the encryption unit 35, the image with obfuscated zone(s) 75 and the encrypted message. The reception module 60 is further configured to receive, from the transmission device 25, and more particularly from the configuration unit 30, the individual secret key I_s specific to same.

5 The decryption module 62 is configured to apply a decryption algorithm to the encrypted pixel values of the encrypted message on the basis of the individual secret key I_s received, so as to acquire a partially decrypted message.

10 More particularly, the decryption module 62 is configured to use a decryption algorithm using the individual secret key I_s . For example, the decryption module 62 is configured to further use the public master key M_p . The decryption algorithm used depends on the ABE algorithm which was used to generate the individual secret key I_s . The algorithm is e.g. known to each reception module 25, by the reception of the individual secret key I_s .

15 According to one example, the decryption module 62 is configured to apply the decryption algorithm to all the values of the pixels of the encrypted message, i.e. to the content of the second data field or fields in the message. In such case, the decryption module 62 is configured to acquire, for the zone or zones 70 representing one or a plurality of objects that the associated receiver device 25 is authorized to consult, the values of the pixels of the identified zone 70 corresponding to same of the image acquired 37 by the transmitter device 20.

20 For the zones 70 corresponding to objects that the receiver module 25 is not authorized to consult, the decryption algorithm fails to decrypt the pixel values and returns an error message.

25 In a variant, for the zones 70, the values of the pixels obtained following the application of the decryption algorithm are distinct from same of the zones 70 in the acquired image 37. In other words, the values of the pixels corresponding to the zones 70 for which the receiver device 37 is not authorized to consult the object represented, form a noisy signal, e.g. an unintelligible content in the partially decrypted message.

30 It should be then understood that the expression "partially decrypted message" refers to the fact that the application of the decryption algorithm does not necessarily make it possible to decrypt the entire encrypted message but only the parts corresponding to the zone(s) representing the object(s) that the receiver device 25 is authorized to consult.

35 The reconstruction module 64 is configured to reconstruct a partially reconstructed image 77 by replacing, in the image with obfuscated zone(s) 75, the values of the pixels of the zones by the values of the pixels of the corresponding zones in the partially decrypted message.

The partially reconstructed image 77 is such that the zones corresponding to objects that the receiver device 25 is authorized to consult are the same as same 70 of the image 37 acquired by the transmission device 20 from the camera 15. The other zones 70 are not decrypted and thus comprise pixels of value(s) distinct from same in the image captured 37 by the transmission device 20. For example, such values form an unintelligible noisy signal.

An example of a partially reconstructed image 77 obtained by the first receiver device 25A is illustrated in Figure 3. As shown in Figure 3, among the "vehicle", "outline" and "face" objects, only the "vehicle" objects are visible.

Preferentially, the reconstruction module 64 is further configured to transmit the partially reconstructed image 77 to the display screen 67 of said receiver device 25, for the display thereof to the user of said receiver device 25.

According to a variant, the decryption module 62 is configured so that, if the encrypted message received by the reception module 60 comprises, for each zone 70, the third data field, the decryption algorithm is applied only to the pixel values associated with the third data field including a respective first character string indicating an object that said receiver device 25 is authorized to consult, in the encrypted message. According to such variant, the reconstruction module 64 is configured to replace, in the image with obfuscated zone(s) 75, only the values of the pixels of the zone(s) 70 comprising values of the pixels to which the decryption algorithm has been applied.

In the example shown in Figure 1, the configuration unit 30 comprises a first information processing unit e.g. of a first memory 80 and of a first processor 82 associated with the first memory 80. The sending module 40; and, optionally, the acquisition module 42, the determination module 44, and the calculation module 46 are each produced in the form of a software program, or a software brick, which can be run by the first processor 82. The first memory 80 is then apt to store sending software and optionally an acquisition software, a determination software and a calculation software. The first processor 82 is then apt to execute each of said software.

Still in the example shown in Figure 1, the encryption unit 35 comprises a second information processing unit e.g. of a second memory 85 and of a second processor 87 associated with the second memory 85. The acquisition module 50, the application module 52, the generator module 54 and the transmitter module 56 are each implemented in the form of a software program, or a software brick, which can be run by second the processor 87. The second memory 85 is then apt to store a receiver software, an application software, a generation software and a transmission software. The second processor 87 is then apt to execute each of said software.

In the example shown in Figure 1, each receiver device 25 comprises a third information processing unit consisting e.g. of a third memory 90 and of a third processor 92 associated with the third the memory 90. In the receiver module 60, the decryption module 62 and the reconstruction module 64 consist each of a software, or a software brick which can be executed by the processor 92. The third memory 90 is then apt to store a reception software, a decryption software and a reconstruction software. The third processor 92 is then apt to execute each of said software.

In a variant (not shown), at least one among the sending module 40, the acquisition module 50, the application module 52, the generator module 54, the transmitter module 56, the receiver module 60, the decryption module 62, the reconstruction module 64 and, optionally, the acquisition module 42, the determination module 44, the calculation module 46 is produced in the form of a programmable logic component, such as an FPGA (Field Programmable Gate Array), or further in the form of a dedicated integrated circuit, such as an ASIC (Application Specific Integrated Circuit).

When the configuration unit 30, the encryption unit 35 and each receiver device 25 is produced in the form of one or a plurality of software programs, i.e. in the form of a computer program, same are further apt of being recorded on a computer-readable medium (not shown). The computer-readable medium is e.g. a medium apt to store the electronic instructions and to be coupled to a bus of a computer system. As an example, the readable medium is an optical disk, a magneto-optical disk, a ROM memory, a RAM memory, any type of non-volatile memory (e.g. EPROM, EEPROM, FLASH, NVRAM), a magnetic card or an optical card. A computer program containing software instructions is then stored on the readable medium.

The operation of the communication system 10 will now be described.

Firstly, the operation of the transmitter device 20 will be described with reference to Figure 5 representing a flow chart of a transmission method 100 according to the invention.

The transmission method 100 comprises a configuration phase 110 and an encryption phase 120.

Preferentially, the configuration phase 110 is implemented prior to the encryption phase 120.

Initially, an operator of the sending device 20 creates the lookup table and sends same to the configuration unit 30.

Optionally, the configuration phase 110 comprises an acquisition step 112 during which the acquisition module 42 acquires the lookup table from the operator.

Optionally, the configuration phase 110 comprises a determination step 114 during which the determination module 44 determines the master public key M_p and the master secret key M_s , e.g. randomly.

Optionally again, the configuration phase 110 then comprises a step 116 of calculating the individual secret keys I_s specific to each receiver device 25, from the lookup table indicating, for each receiver device 25, the object or objects that same is authorized to consult. Preferentially, each individual secret key is calculated on the basis of the master secret key M_s , from the objects of the lookup table, and from an ABE algorithm as described hereinabove.

The configuration phase 110 further comprises a step 118 of sending, to each receiver device 25, the individual secret key I_s specific to same. For this purpose, the sending module 70 preferentially uses a secure channel such as the TLS type, such as an HTTPS channel that is encrypted and authenticated.

In a variant, each individual secret key I_s is already stored in the configuration unit 30. According to such variant, the configuration phase 110 comprises only the sending step 118.

The encryption phase 120 comprises a step 121 of acquiring the image 37 comprising at least one zone 70 identified as representing an object, respectively.

The acquiring step 121 preferentially comprises a sub-step 122 of acquisition, from the camera 15, of the image 37.

Then, the acquiring step 121 preferentially comprises a sub-step 123 of identifying, in the acquired image 37, the zones 70 representing each object.

For example, during the identification sub-step 123, the acquisition module 50 applies, to the acquired image 37, the identification model including the neural network described hereinabove, in order to identify each zone 70.

The encryption phase 120 further comprises an application step 124, during which the application module 52 applies, to each identified zone 70, the obfuscation, so as to form the image with obfuscated zone(s) 75. The image with obfuscated zone(s) 75 comprises, in each identified zone 70, pixels, a value of which is distinct from the value of the same pixels in the acquired image 37.

The encryption phase 120 further comprises step 125 of generating an encrypted message.

The generation step 125 preferentially comprises a storage sub-step 126 and a sub-step of applying an encryption 127.

During the storage sub-step 126, the generator module 54 stores, for each identified zone 70, the values of the pixels of the acquired image 37, in the message. The message is preferentially a database.

Advantageously, the message then comprises, for each identified zone 70 in the acquired image 37: the first data field including the position of said zone 70 in the acquired image 37 and the second data field including the values of the pixels in the acquired image 37. For each identified zone 70, the first data field is preferentially arranged, in the message, before the second data field.

During the sub-step of applying the encryption 127, the generator module 54 applies the encryption to the values of the pixels of the message on the basis of the master public key M_p and of the encryption policy, as indicated hereinabove.

At the end of the sub-step of applying the encryption 127, all the values of the pixels of the message are encrypted, thereby forming the encrypted message.

The encryption phase 120 further comprises a transmission step 128 during which the transmission module 56 transmits, to each receiver device 25, the image with obfuscated zone(s) 75 and the encrypted message.

For example, the encrypted message is comprised in the metadata of the image with obfuscated zone(s) 75.

The transmission step 128 is performed e.g. via a standard, non-secure communication channel.

For example, all the steps 121, 124, 125, 128 of the encryption phase 120 are reiterated for a plurality of images 37 forming a video stream. Thereby, for each image 37 of the video stream, the encryption unit 35 successively implements each of the steps of acquiring 121, applying 124, generating 125 and transmitting 128.

According to another example, for each image 37 forming the video stream, the encryption unit successively implements only the steps of acquiring 121, applying 124 and generating 125. The encryption phase 120 then comprises a single transmission step 128 for all of the images with obfuscated zone(s) 75 and of the associated encrypted messages.

The configuration phase 110 and the encryption phase 120 are e.g. implemented successively as described hereinabove.

According to an alternative, the configuration phase 110 and the encryption phase 120 are implemented in parallel. In such case, it is nevertheless preferable for the determination step 114 to be implemented prior to the generation step 125 so that during the application sub-step 127, the master public key M_p has already been determined.

According to the invention, the operation of each receiver device 25 will be described with reference to Figure 6 describing a reception method 200 implemented by each receiver device 25.

The reception method 200 comprises a reception step 210. The reception module 60 receives, from the transmitter device 20, the individual secret key I_s specific to same, the image with obfuscated zone(s) 75 and the encrypted message during the reception step 210.

According to the invention, the reception 210 of the individual secret key I_s and the reception of the image with obfuscated zone(s) 75 are preferentially not performed at the same instants.

Advantageously, the reception module 60 receives the individual secret key I_s specific to same, from the sending module 40 via the secure channel.

For example, the reception module 60 receives the image with obfuscated zone(s) 75 and the encrypted message from the transmission module 56, via the non-secure channel.

The individual secret key I_s is received before or after the image with obfuscated zone(s) 75 and the encrypted message.

Preferentially, the encrypted message is a database.

The reception method 200 then comprises a decryption step 220 during which the decryption module 62 applies the decryption algorithm to the encrypted message, on the basis of the individual secret key I_s , received, so as to acquire the partially decrypted message.

For example, the decryption module 62 applies the decryption algorithm to all the values of the encrypted pixels of the encrypted message.

During the decryption step 220, the application of the decryption algorithm makes it possible to acquire, for the identified zone or zones 70 representing an object that the receiver device 25 is authorized to consult, the values of the pixels of said zones 70 in the acquired image 37. For the other zone(s), where appropriate, the application of the decryption algorithm provides pixel values distinct from same in the acquired image 37.

In other words, the application of the decryption algorithm makes it possible to decrypt only the values of the pixels of the zone or zones 70 representing the object or objects that the receiver device 25 is authorized to consult. For the pixel values of the other zone(s) 70, the application of the decryption algorithm provides pixel values that do not represent any intelligible content.

The decryption method 200 then comprises a reconstruction step 230 during which the reconstruction module 64 reconstructs the partially reconstructed image 77. For this

purpose, the reconstruction module 64 replaces, in the image with obfuscated zone(s) 75, the values of the pixels of the obfuscated zone(s) with the values of the corresponding pixels of the partially decrypted message, so as to form the partially reconstructed image 77.

Preferentially, during the replacement step 230, the reconstruction module 64 sends
5 the partially reconstructed image 77 to the display screen 67 of the receiver device 25.

Thereby, the user of the receiver device 25 consulting the partially reconstructed image 77 has access only to the objects of the acquired image 37 that the user is authorized to consult, the other object or objects not being represented in the partially reconstructed image 77.

10 The reception method 200 is e.g. iterated for a plurality of images with obfuscated zone(s) 77 and associated encrypted messages. The individual secret key I_s is preferentially received only once.

According to a first variant, the encrypted message further comprises, for each identified zone 70, the third data field comprising the first character string indicating the
15 object represented in said zone 70. For example, if a zone 70 represents a face, the encrypted message comprises the first data field indicating the position of that zone in the acquired image. the third data field including the first character string "face" and the second data field comprising the values of the pixels of said zone 70 which have been encrypted.

According to the first variant, during the decryption step 220, the decryption module
20 62 applies the decryption algorithm only to the values of the pixels associated with the third data field including a string of characters corresponding to an object that the receiver device 25 is authorized to consult.

Still according to the first variant, during the replacement step 230, the reconstruction module 64 replaces, in the image with obfuscated zone(s) 75, only the pixels
25 of zone(s) 70 for which the decryption algorithm has been applied by the decryption module 62. According to such variant, the zone or zones of the partially reconstructed image 77 distinct from the zone or zones representing an object that the receiver device 25 is authorized to consult, are identical to the zones of the image with obfuscated zone(s) 75.

According to a second variant, the reception module 60 receives a plurality of
30 images with obfuscated zone(s) 75 and the corresponding encrypted messages before implementing the decrypting 220 and the reconstruction 230 steps. According to the second variant, the individual secret key I_s is e.g. received before and/or after the reception of all the images with obfuscated zone(s) 77 and corresponding encrypted messages.

According to a third variant (not shown), the communication system 10 comprises a
35 plurality of cameras 15. According to the third variant, each individual secret key I_s is apt to

decrypt only the values of the pixels corresponding to a zone 70 representing one or a plurality of objects and coming from one or a plurality of chosen cameras 15.

For example, the communication system 10 comprises a first camera 15 taking images in front of a first parking entrance, and a second camera 15' taking images in front of a second parking entrance. The communication system 10 comprises a first receiver device 25A associated with a first security guard watching over the first entrance and a first receiver device 25A' associated with a second security guard watching over the second entrance.

In the present example, the first receiver device 25A associated with the first security guard is authorized to consult only the "vehicle" objects captured on image by the first camera 15, whereas the first receiver device 25A' associated with the second security guard is authorized to consult only the "vehicle" objects captured on image by the second camera 15'.

According to the optional supplement wherein the configuration unit 30 comprises the acquisition module 42, the determination module 44 and the calculation module 46, the lookup table then associates, with each receiver device 25, the list of respective object(s) and for each object, the camera or cameras 15 from which come the images 37 representing the object. Thereby, in the present example, the lookup table associates:

- the "vehicle" object coming from the first camera 15, 15', with the first receiver device 25A associated with the first security guard,
- the object "vehicle" coming from the second camera 15, 15', with the first receiver device 25A' associated with the second security guard
- the object "outline" coming from each camera 15, 15', with the second receiver device 25B associated with the police department, and
- the objects "vehicle", "outline" and "face" coming from each camera 15, 15', with the third receiver device 25C associated with the examining magistrate.

The calculation module 46 is then configured to calculate each individual secret key I_s depending on the list of object(s) and also on the camera 15, 15' from which the image 37 comes.

The acquisition module 50 is configured to acquire at least one respective image 37 from each camera 15, 15', each image 37 having one or a plurality of identified zones 70.

The application module 52 is then configured to apply the masking to each identified zone 70 of each image 37.

The generator module 54 is configured for generating a respective encrypted message for each image 37.

Alternatively, the generator module 54 is configured to generate a single encrypted message for a set comprising an image 37 coming from each camera 15, 15'. Each logical relation of the encryption policy then combines the object or objects represented in the identified zone 70 and a context element which is the camera 15, 15' from which comes the image 37 associated with the identified zone 70.

The transmitter module 56 is configured to transmit, to each receiver device 25, each image with obfuscated zone(s) 75 and the or each encrypted message.

According to the third variant, the decryption module 62 is configured to then apply, if the reception module 60 has received an encrypted message for each image with obfuscated zone(s) 75, the decryption algorithm to each encrypted message corresponding to a camera 15, 15' for which the receiver device (25) is authorized to consult at least one object. The decryption module 62 is configured to then apply, if the reception module 60 has received only one encrypted message for all the images with obfuscated zone(s) received 75, the decryption algorithm only to the values of the pixels for which the individual secret key I_s is associated with at least one object and/or context element(s) verifying the logical relation of the third data field.

According to such variant, the reconstruction module 64 is configured, if a message encrypted by image with obfuscated zone(s) 75 is received, to replace the values of the pixels of each obfuscated zone of each received image 75 by the values of the pixels of the associated partially decrypted message.

The reconstruction module 64 is configured, if an encrypted message is received for all the images with obfuscated zone(s) 75, to replace in each image with obfuscated zone(s) 75, the values of the pixels of each obfuscated zone by the values of the decrypted pixels of the partially decrypted message.

According to the third variant, the transmission method is identical to the transmission method 100 described hereinabove, except for the following differences.

During the optional calculation step 116, the calculation module 46 calculates the individual secret key I_s associated with each receiver device 25, also taking into account the camera or cameras 15 for which the receiver device 25 is authorized to consult the objects.

During the acquiring step 121, the acquisition module 50 acquires a respective image 37 with one or a plurality of identified zones 70, for each camera 15, 15'. Preferentially, the acquiring step 121 comprises the acquisition 122 and identification 123 sub-steps which are implemented for each image 37.

The application step 124 is applied to each image 37 so as to form, for said image 37, an image with respective obfuscated zone(s) 75.

During the generation step 125, the generator module 54 generates a respective encrypted message per image 37 as described hereinabove, or an encrypted message for all the images 37. In the latter case, the third data field of the encrypted message then comprises the logical relationship associated with the object(s) represented in the identified zone 70 and with the context element(s) of the encryption policy.

During the transmission step 128, the transmitter module 56 transmits, to each receiver device 25, the images with obfuscated zone(s) 75 and the encrypted message(s).

The reception method 200 according to such variant of embodiment is identical to the reception method 200 described hereinabove, except for the following differences.

During the reception step 210, the reception module 60 receives each image with obfuscated zone(s) 75 and the encrypted message(s).

The decryption step 220 is implemented for the or each encrypted message so as to acquire one or a plurality of partially decrypted messages.

If an encrypted message for each image with obfuscated zone(s) 75 has been received, the reconstruction step 230 is iterated for each partially decrypted message, i.e. for each image with obfuscated zone(s) 75.

If an encrypted message has been received for all the images with obfuscated zone(s) 75, during the reconstruction step 230, the reconstruction module 64 replaces, for each image with obfuscated zone(s) 75, the pixel values of each zone obfuscated by the decrypted pixel values of the partially decrypted message.

The first and second variants described hereinabove can be combined with the third variant described hereinabove.

With the transmission method 100 according to the invention, it is possible to transmit an image which protects the personal data, while being partially decryptable for a user authorized to consult part of the content thereof.

With the reception method 200 according to the invention, it is possible to decrypt only a part of an image for which only certain objects are authorized to be consulted.

Thereby, the transmission (100) and reception (200) methods according to the invention make it possible to improve the confidentiality of personal data.

23
CLAIMS

1. A method of transmission (100), from an electronic transmitter device (20) to at least one electronic receiver device (25), an image (37) representing at least one object,
5 the transmission method (100) being implemented by the electronic transmission device (20) and comprising a configuration phase (110) including the following step:

- acquisition (112) of a lookup table, the lookup table associating with each electronic receiver device (25) a respective list of object(s) that said electronic receiver device (25) is authorized to consult by decrypting the encrypted message, on the basis of said individual secret key (I_s),
10
- determination (114) of a master public key (M_p) and of a master secret key (M_s),
- calculation (116), for each electronic receiver device (25), of the respective individual secret key (I_s) from the master secret key (M_s) and the list of object(s) associated with said electronic receiver device (25) in the lookup table,
15
- sending (118) to the or each electronic receiver device (25) a respective individual secret key (I_s),

the method (100) further comprising an encryption phase (120) including the following steps:

- acquiring (121) the image (37) representing the at least one object, wherein one or a plurality of zones (70) including certain pixels of the image are identified, each identified zone (70) representing the or at least one object,
20
- applying (124) an obfuscation to the or each zone (70) of the image (37), so as to form an image with obfuscated zone(s) (75),
- generating (125) an encrypted message comprising pixel values of the zones in the resulting image, wherein said values are encrypted, the pixel values being encrypted on the basis of the master public key (M_p),
25
- transmitting (128) to the or each electronic receiver device (25), the image with obfuscated zone(s) (75) and the encrypted message for at least partial decryption, by each electronic receiver device (25) in order to reconstruct a partially reconstructed image (77) associated with the electronic receiver device (25),
30

wherein each individual secret key (I_s) is calculated from the lookup table by applying a key generation function of an attribute encryption algorithm.

2. The method (100) according to claim 1, wherein the acquiring step (121) comprises the following sub-steps:

- acquisition (122) of the image (37), and
- identification (123) in the acquired image of zone(s) (70) representing the or each object from an identification model,

the identification step (123) being preferentially implemented by an identification model comprising more preferentially a neural network.

3. The method (100) according to claim 1 or 2, wherein the generation step (125) comprises the following sub-steps:

- storage (126), in a message, of pixel values corresponding to the zone(s) identified in the image,
- application (127) of an encryption algorithm to the values of the pixels of the message from the master public key (M_p), so as to form the encrypted message,

the encryption algorithm being preferentially chosen from the group consisting of:

- the BSW07 algorithm,
- the CPW08 algorithm, and
- the AC17 algorithm

4. The method (100) according to any of the preceding claims, wherein the obtained image (37) comes from a camera (15, 15') chosen from a predefined list of cameras (15, 15'), the lookup table associating, for each electronic receiver device (25), for each object, one or a plurality of cameras (15, 15') suitable for taking images for which the electronic receiver device (25) is authorized to consult said object,

the or each individual secret key (I_s) further depending on the camera or cameras (15, 15') associated with the corresponding electronic receiver device (25) in the lookup table.

5. A computer program product comprising software instructions which, when executed by a computer, implement a reception method (100) according to any of the preceding claims.

6. An electronic transmitter device (20) for transmitting to at least one electronic receiver device (25), an image (37) representing at least one of object among a predefined list of objects, the electronic transmitter device (25) comprising a configuration unit (30) comprising:

- an acquisition module (42) configured to acquire a lookup table, the lookup table associating with each electronic receiver device (25), a respective list of object(s) that said electronic receiver device (25) is authorized to consult by decrypting the encrypted message, on the basis of said individual secret key (I_s),
- 5 - a determination module (44) configured to determine a master public key (M_p) and a master secret key (M_s), and
- a calculation module (46) configured to calculate the respective individual secret key (I_s) from the master secret key (M_s) and from the list of object(s) associated with said electronic receiver device (25) in the lookup table,
- 10 - a sending module (40) configured to send to the or each electronic receiver device (25), a respective individual secret key (I_s),

the electronic transmission device (20) further comprising at least one decryption unit (35) including:

- an acquisition module (50) configured to acquire the image (37) representing the
- 15 at least one object, wherein one or more zones (70) including certain pixels of the image are identified, each identified zone (70) representing the or one of the objects,
- an application module (52) configured to apply a masking to the or each zone (70) of the image (37), to form an image with obfuscated zone(s),
- 20 - a generator module (54) configured to generate an encrypted message comprising values of pixels of the zones (70) in the obtained image (37), wherein said values are encrypted, the values of the pixels being encrypted from a master public key (M_p),
- a transmission module (56) configured to transmit, to each electronic receiver
- 25 device (25), the image with obfuscated zone(s) (75) and the encrypted message for at least the partial decryption thereof, by each electronic receiver device (25), so as to reconstruct a partially reconstructed image (77) associated with the respective electronic receiver device (25),

wherein each individual secret key (I_s) is calculated from the lookup table by applying a key generation function of an attribute encryption algorithm.

7. A method of reception (200), by an electronic receiver device (25) and from an electronic transmitter device (20), of an image (75) with at least one obfuscated zone suitable for representing an object from a predefined list of object(s),

35 the method (200) being implemented by an electronic receiver device (25) and comprising the following steps:

- reception (210) of the image with obfuscated zone(s) (75), of an encrypted message comprising encrypted pixel values, and of an individual secret key (I_s) associated with the electronic receiver device (25),
the individual secret key (I_s) being suitable for decrypting only the encrypted pixel values corresponding to one or a plurality of zones of the image with obfuscated zone(s) (75) representing objects which the electronic receiver device (25) is authorized to consult,
- decryption (220), on the basis of a decryption algorithm and the received individual secret key (I_s), of the encrypted pixel values of the encrypted message, so as to acquire a partially decrypted message, and
- reconstruction (230) of a partially reconstructed image (77), by replacing the obfuscated zone(s) of the image with obfuscated zone(s) (75) by pixels the values of which are comprised in the partially decrypted message,

at least one zone of the partially reconstructed image (77) representing an object that the electronic receiver device (25) is authorized to consult.

8. A computer program comprising software instructions which, when executed by a computer, implement a reception method (200) according to the preceding claim.

9. An electronic receiver device (25) for receiving, from an electronic transmitter device (20), an image (75) with at least one obfuscated zone suitable for representing an object,
the electronic reception device (25) comprising:

- a reception module (60) configured to receive the image with obfuscated zone(s) (75), an encrypted message comprising encrypted pixel values, and an individual secret key (I_s) associated with said electronic receiver device (25),
the individual secret key (I_s) being apt to decrypt only the encrypted pixel values corresponding to one or a plurality of zones of the image with obfuscated zone(s) (75) representing objects that the electronic receiver device (25) is authorized to consult,
- a decryption module (62) configured to decrypt, from a decryption algorithm and the received individual secret key (I_s), the encrypted pixel values of the encrypted message in order to acquire a partially decrypted message, and
- a reconstruction module (64) configured to reconstruct a partially reconstructed image (77) by replacing the obfuscated zone(s) of the image with obfuscated

zone(s) (75) by pixels the values of which are comprised in the partially decrypted message,

at least one zone of the partially reconstructed image (77) representing an object that the electronic receiver device (25) is authorized to consult.

5

10. An electronic communication system (10) comprising an electronic transmitter device (20) and at least an electronic receiver device (25), wherein the electronic transmitter device (20) is according to claim 6 and each electronic receiver device (25) is according to claim 9.

10