The present invention will further be explained below with reference to exemplary embodiments illustrated in the accompanying drawings, in which:

Fig. 1 (a) and (b) schematically shows token shares creation and storage process according to the present invention;

Fig 2 illustrates the token shares decryption process according to the present invention;

Fig 3 illustrates the modified F5 algorithm in accordance with the present invention;

~~Fig 4 illustrates the QR Login sequence diagramin accordance with the present invention;~~

Fig 5 illustrates the QR Shop payment transaction sequence diagramin accordance with the present invention;

Fig 6 illustrates the block diagram showing secure mobile shopping process in accordance with the present invention;

~~Fig 7 illustrates the Live Sequence Chartsin accordance with the present invention;~~

DETAILED DESCRIPTION

The present patent application relates to an innovative use of Cryptographic tokens (keys) generated out of a hardware based True Random Number Generator, Statistical tests to weed out weak keys, number-to-image transformation, new steganographic methods of injecting into a Image carrier and splitting into shares using Visual Cryptographic methods and using it with a configured mobile application for real time product verification and seamless secured shopping. The present disclosure is not restrictive just for the whole process flow and also for the tokens generated thereupon for distribution in smartcard media or USB flash drives or in smart mobile applications and /or as computer program product.. The total flow of work is depicted in Fig [1a and Fig 1b] with illustrations.

The TRNG (True Random Number Generator) is implemented using FPGA based generator built with a Thermal Noise Generator. The hardware appliance generates continuous keys of required lengths. The keys generated are sieved through statistical tests and are orthogonal amongst the created are only good candidates are chosen as tokens or Keys.

CLAIMS:

1. A method of generating secure tokens and transmission based on ~~(TRNG)~~ True Random Number Generator generated tokens and split into shares, the method comprising steps of:

generating the keys by a hardware based True Random number Generator ~~(TRNG)~~ ;

sieving / filtering the generated keys using statistical tests suite and are orthogonal amongst the created;

selecting the random numbers of required width as tokens;

applying number to image transformation for the said tokens;

applying steganography methods of injecting into image carrier to the selected tokens; and

splitting the steganographic contents into at least two shares using Share Generation Appliance, which is based on visual cryptographic methods.

2. The method as claimed in claim 1, wherein the key generation appliance is based on FPGA based generator build with a Thermal noise generator with frequencies preferably 1 to 6 MHZ.

3. The method as claimed in claim 1, wherein Von Neumann method is applied to generated keys which include discarding them under condition that the two sample key bits are equal and accumulating one of the key bits if they are not equal.

4. The method as claimed in claim 1, wherein there is a closed loop link between generation process and statistical testing suite of Die-Hard to quantify the usable frequencies for ~~(TRNG)~~ True Random Number Generation number generation.

5. The method as claimed in claim 1, wherein the splitting of the shares contains partial information about the secret.

6. The method as claimed in claim 1, wherein for every key, a pair of share tokens is created.

7. The method as claimed in claim 1, wherein, the either shares contains no full information on the original image because of the randomization and the original image is revealed under condition that the shares gets physically overlaid and are fit together.

8. The method as claimed in claim 7, wherein, under condition that either share do not fit together, then no information on the original image is revealed and a random image is produced.

9. A system of generating secure tokens and transmission based on ~~(TRNG)~~ True Random Number Generator generated tokens and split into shares, the system comprising of:

means for generating the keys by a hardware based True Random number Generator ~~(TRNG)~~;

means for sieving / filtering the generated keys using statistical tests suite;

means for selecting the random numbers of required width as tokens;

means for applying number to image transformation for the said tokens;

means for applying steganography methods of injecting into a image carrier to the selected tokens; and

means for splitting the steganographic contents into at least two shares using visual cryptographic methods.

10. The system as claimed in claim 9, wherein the key generation appliance is based on FPGA based generator build with a Thermal noise generator with frequencies preferably 1 to 6MHZ.