What is claimed is:

1. A computer-implemented method for certifying a security document, comprising:

providing a security document which is the result of a plurality of independent manufacturing processes that provides each a feature, said security document having a set of unique characteristics related to variations in the relative positions of the features which vary from document to document due to the intrinsic variability of the manufacturing processes as well as the variations due to the use of different raw materials for manufacturing the security document;

obtaining, via the one or more computer processors, a digital image of the security document;

selecting, via one or more computer processors, a determined set of locations from the document features; and obtaining a variety of measurements regarding the relative positions of the features of the document;

constructing, via the one or more computer processors, a message from said measurements of relative positions acquired from the determined set of locations of the document;

constructing, via the one or more processors, a hashed message, wherein the hashed message is obtained by encoding the message with a unidirectional cryptographic hash function,

encrypting, via the one or more processors, the hashed message using a private key, by a public key cryptographic system, to obtain a digital certificate, and

storing, via the one or more processors, the digital certificate in an external database.

2. The method for certifying a security document according to Claim 1, wherein the digital certificate is marked or printed on the security document.

3. The method for certification according to Claim 1 wherein the digital image is taken with light with a wavelength between 200 and 1500 nanometers.

4. The method for certification according to Claim 1 wherein the digital image is taken with visible light.

5. The method for certification according to Claim 1 wherein many parts of the same document are independently certified.

6. A method for certification according to Claim 1, wherein the security document is a banknote, a check, a passport, visa, ID document or birth certificate.

7. The method for certifying a security document according to Claim 1, wherein the data of the set of unique characteristics related to variations in the relative positions of the features which vary from document to document is obtained throughout a production line of security documents.

8. The method for certifying a security document according to Claim 1, wherein the data of the set of unique characteristics related to variations in the relative positions of the features which vary from document to document, is obtained during quality inspection.

9. A computer-implemented method for the authentication of a certified security document, comprising the steps of:

providing, via one or more processors, a security document to be authenticated;

verifying, via the one or more processors, that the genuine security raw materials and manufacturing processes are present in the security document,

obtaining, via the one or more computer processors, a digital image of the security document and obtaining the measurements of the relative positions of the features incorporated during the manufacturing processes from the determined set of locations of the document image;

constructing, via the one or more processors, a message by measuring the register of the selected one or more features from the security document and from document ID data,

applying a hash function to the message to obtain a hashed message for verification,

retrieving, via the one or more processors, and decrypting the ~~stored~~ digital certificate to obtain the certified hashed message for the security document;

authenticating, via the one or more processors, the document by comparing the certified hashed message and the hashed message for verification, where if the

certified hashed message and the hashed message for verification are a match, the document is considered as genuine, and if the certified hashed message and the hashed message for verification do not match, the document is considered as a counterfeit.

10. The method for the authentication of a security document according to Claim 9, wherein the certified hashed message is obtained from the digital certificate marked or printed on the security document, and the digital certificate is decrypted through the use of a public key to render the certified hashed message for reference.

11. The method for the authentication of a security document according to Claim 9, wherein the certified hashed message is obtained by accessing the database.

12. The method for authenticating according to Claim 9, wherein the raw materials are verified via image analysis and pattern recognition methods.

13. The method for authentication according to Claim 9, wherein the security document is a banknote.

14. The method for authentication according to Claim 9, wherein the security document is a banknote and the features incorporated by manufacturing processes comprising at least one the following: a watermark, a security thread, a foil, a transparent window or fluorescent fibers or an image from a printing process.

15. The method for authentication according to Claim 9, wherein the printing process includes at least offset printing or intaglio printing.

16. The method for the authentication of a security document according to Claim 9, wherein the authentication is performed by commercially available scanners or digital cameras connected to computers.

17. The method for the authentication of a security document according to Claim 9, wherein the authentication is performed by smart phones or tablets.

18. The method for the authentication of a security document according to Claim 9, wherein the authentication is performed by cash processing equipment.