CLAIMS:

1. A method of generating secure tokens and transmission based on (TRNG) 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 (SGA), 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 (keys) bits are equal and accumulating one of the bits (keys) if they are not equal. .

~~4. The method as claimed in claim 1, wherein the generated numbers (keys) under condition that they don't undergo the Die-Hard Test suite then the appropriate frequency of generation is dropped.~~

~~5.~~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 number generation.

~~6.~~5. The method as claimed in claim 1, wherein the splitting of the shares contains partial information about the secret.

~~7.~~6. The method as claimed in claim 1, wherein for every key, a pair of share tokens is created.

~~8. The method as claimed in claim 1, wherein, one share token, the stegano content (Carrier and the TRNG key number) and the original cryptograpic key is stored at server level, including the procedures for reversing steganographic procedure, combining procedure for getting back the original number out of the two shares using Visual cryptography and verifying with original key.~~

~~9. The method as claimed in claim 1, wherein, the second share token, is stored into media like Smart cards, USB flash drives, with or without biometric fingerprint scanner or any other media as per PKCS#11 standards of key distribution.~~

~~10.~~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.

~~11.~~8. The method as claimed in claim 10, 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.

~~12. The method as claimed in claim 1, wherein, the share token is the stego message and is embedded in the cover image (Implemented as Logo Images of Different Enterprises) before the activation of Visual cryptography algorithm is initiated using a modified F5 algorithm.~~

13. The method as claimed in claim 12, wherein any event of hacking or breach would only reveal the Logo of the enterprise rather than the associated TRNG Token within it.

14. The method as claimed in claim 12, wherein the Logo with the embedded token is split using non-linear algorithm of splitting into two or more shares and the different Non-linear algorithms results in different pairs of orthogonally different numbers of shares (two or more depending on the splitting methods).

15. The method as claimed in claim 1, wherein, the F5 algorithm embeds message bits into randomly-chosen OCT coefficients and employs matrix embedding that minimizes the necessary number of changes to embed a message of certain length including inputs as:

Quality factor of the stego-image Q;
Input file (TIFF, BMP, JPEG, or GIF);
Output file name;
File containing the secret message;
User password to be used as a seed for PRNG;
Comment to be inserted in the header.

16. The method as claimed in claim 15, wherein, the matrix embedding has three parameters (c, n, k), where c is the number of changes per group of n coefficients, and k is the number of embedded bits including simple matrix embedding (1, 2k-1, k) using a "hash" function that outputs k bits when applied to 2k-1 coefficients.

17. The method as claimed in claim 16, wherein, the embedding process includes the steps of:

selecting the RGB representation of the input image;
calculating the quantization table corresponding to quality factor Q and compressing the image while storing the quantized OCT coefficients;

computing the estimated capacity with no matrix embedding;

generating a seed for a PRNG using a user-specified password that determines the random walk for embedding the message bits; wherein the message is divided into segments of k bits that are em_bedded into a group of 2k-1 coefficients along the random walk and under condition that the hash of that group does not match the message bits, the absolute value of one of the coefficients in the group is decreased by one to obtain a match and if the coefficient becomes zero, the same k message bits are re-embedded in the next group of OCT coefficients (LSB(d)= d mod 2, for d > 0, and LSB(d)=1- d mod 2, for d < 0) and further if the message size fits .the estimated capacity, the embedding proceeds, otherwise an error message showing the maximal possible length is displayed.

18. The method as claimed in claim 17, wherein the step of computing is carried out with following equation:

$$C = hDCT - hDCT/64 - h(O) - h(1) + 0.49h(1),$$

wherehDCT is the number of all OCT coefficients, h(O) is the number of AC OCT coefficients equal to zero, h(1) is the number of AC OCT coefficients with absolute value 1, hDCT/64 is the number of DC coefficients, and -h(1)+0.49h(1) = -0.51h(1) is the estimated loss due to shrinkage and the parameter C and the message length together determine the best matrix embedding.

19. The method as claimed in claim 17, wherein the PRNG also generates a pseudo-random bit-stream that is XOR-ed with the message to make it a randomized bit stream.

20. The method as claimed in claim 17, wherein during the process of embedding, DC coefficients and coefficients equal to zero are skipped.

21. The method as claimed in any of the preceding claims further comprising the step of verifying the keys at the server level.

~~22. The method as claimed in claim 21, wherein, during verification of the keys at server level, two level authentication is carried out wherein at the first level when the reconstructed image of the two shares reveals the Stegano carrier Image and second, the original TRNG value gets reconstructed after dispensing the stegano carrier.~~

5 .

~~23. The method as claimed in any of the preceding claims wherein the shares generated are as equivalent to PKI certificates generated and no third party required to be involved is such shares (tokens) generation unlike in conventional certificate/Tokens/Key generation process.~~

10

~~24. The method as claimed in claim 21, wherein in the verification process from the shares the Image processing methods are applied for cleaning the salt and pepper noise after overlaying the shares and doing a raster to vectorization process to get back the ASCII value from the raster content, to reconstruct the token and compare with the~~

~~15 original:~~

~~25.~~9. A system of generating secure tokens and transmission based on (TRNG) generated tokens and split into shares, the system comprising of:

means for generating the keys by a hardware based True Random number

. 20 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

25 the selected tokens; and

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

~~26.~~10. The system as claimed in claim ~~25~~ 9, wherein the key generation appliance is

30 based on FPGA based generator build with a Thermal noise generator with frequencies preferably 1 to 6MHZ.

27. The system as claimed in any of the preceding claims, wherein the shares generated are as equivalent to PKI certificates generated and no third party required to be involved is such shares (tokens) generation unlike in conventional certificate/Tokens/Key generation process.

28. The system as claimed in any of the preceding claims, wherein in the event of hacking or breach the step would only reveal the Logo of the enterprise rather than the associated TRNG Token within it.

29. The system as claimed in claim 25, further comprising means for verifying the keys at the server level.

30. The system as claimed in claim 25, wherein, one share token, the stegano content and the original cryptographic key is stored at server level, including the procedures for reversing steganographic procedure, combining procedure for getting back the original number out of the two shares using Visual cryptography and verifying with original key and the second share token, is stored into media like Smart cards, USB flash drives, with or without biometric fingerprint scanner or any other media as per PKCS#11 standards of key distribution.

31. A method of secured shopping using a mobile by generating secure tokens and transmission based on (TRNG) 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 a image carrier to the selected tokens;

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

pasting one share on the product meant for the shopping as QR code; and

storing the other share in the verification server; wherein the verification of the shares is carried out at server level with the reconstructed image of the two shares revealing the Stegano carrier Image and the original TRNG value getting reconstructed after dispensing the stegano carrier.

32. A method of secured shopping using a mobile as claimed in claim 31 further comprising the steps of :

registering the consumer I user with a website for receiving exclusive login credentials;

logging by the user in the said website with registered credentials;

adding the user device to the website; and

installing the mobile application software in the consumer/user mobile.

33. A method of secured shopping using a mobile as claimed in claim 31 further comprising the steps of :

entering the username and password in mobile as website credentials for one time;

choosing a PIN for further mobile authentication, once the credentials are accepted by the website; and

adding the mobile unique ID to list of devices for the user account.

34. A method of secured shopping using a mobile as claimed in claim 31 wherein the step of verification further comprising the steps of :

entering by the consumer/ user, the credentials in the browser, which then displays QR code;

scanning the QR code present over the product and entering the mobile application PIN; wherein

under condition that the QR and PIN are valid, then the user login page is displayed in browser.

35. A method of secured shopping using a mobile as claimed in claim 31 wherein the website can be a bank website, financial website, e-shopping website, and the like.

36. A method of secured shopping using a mobile as claimed in claim 31 further includes a payment gateway for payment transactionsand is carried out by splitting the steganographic contents into three shares using Share Generation Appliance ((SGA), which is based on visual cryptographic methods.

37. A method of secured shopping using a mobile as claimed in claim31, wherein a valid. payment transaction is done with server authentication, user authentication and Payment Gateway (PG) Authentication.

38. A system for secured shopping using a mobile by generating secure tokens and transmission based on (TRNG) 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 visualcryptographic methods; wherein one share is pasted on the product meant for the shopping as QR code and the other share is stored in the verification server; wherein the verification bf the shares is carried out at server level with the reconstructed image

of the two shares revealing the Stegano carrier Image and the original TRNG value getting reconstructed after dispensing the stegano carrier.

39. The system as claimed in claim 38, wherein the shares generated are as equivalent to PKI certificates generated and no third party required to be involved is such shares (tokens) generation unlike in conventional certificate/Tokens/Key generation process.

40. The system as claimed in claim 38, wherein in the event of hacking or breach the step would only reveal the Logo of the enterprise rather than the associated TRNG Token within it.