ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 5, May 2017

Video-Object Steganography for Remote Authentication using Adaptive Neuro Fuzzy Inference System

Tani Jaison [1], Sarika K. T [2]

P.G. Student, Department of Electronics and Communication Engineering, Vidya Academy of Science & Technology, P.O. Thalakkottukara, Kerala, India[1]

Assistant Professor, Department of Electronics and Communication Engineering, Vidya Academy of Science & Technology, P.O. Thalakkottukara, Kerala, India[2]

ABSTRACT: In communications, sensitive information are frequently exchanged requiring remote authentication. Remote authentication involves the submission of encrypted signal, along with visual and audio information (facial images/videos, human voice, and so on). Biometric image encryption has emerged as a simple solution for privacy-related applications so that personal biometrical images should not be browsed without permission. Consequently, online biometric verification needs to be carried out in the scrambled domain. The proposed idea is designed in embedded platform with the help of image processing. Raspberry Pi is used for capturing the image of person. The biometric signal which is fingerprint signals captured by fingerprint scanner is embedded within the image of the person. Before hiding the biometric image into facial image, it is scrambled so that no one can able to identify the data. Here biometric signal is encrypted by the chaotic method. Afterwards, the encrypted signal is inserted to the most signicant wavelet coefficients of the Video-object, using its qualified significant wavelet trees(QSWTs). QSWTs provide both invisibility and significant resistance against lossy transmission and compression. Finally, the inverse discrete wavelet transform is applied to provide the stegoobject. Retreived biometric signal is evaluated by minutiae algorithm. Adaptive neural fuzzy inference system helps to store wide variety of databases and more users can interact at a time. The experimental results validated that this method can robustly cope with the challenging tests in the scrambled domain and recognition of the actual user achieving authentication, making this method a promising one for the emerging privacy-related facial biometric applications.

KEYWORDS: Biometrics: biometric image encryption, Chaotic encryption, Minutiae algorithm.

I. INTRODUCTION

Biometrics attributes are unique to every individual thereby used in variety of applications where there is a need to claim the authenticity of an individual [1, 2]. With the rapid transmission of biometric data over the internet, the security of this biometric data is a major concern as sharing and openness in networking environment expose the biometric data to threats. Among various methods encryption is considered to be a potential solution for securing biometric data [3]. Traditional encryption algorithms like RSA, AES and DES are not suitable for securing biometric data due to its intrinsic behaviour like bulky data capacity, high correlation among pixels of biometric data and high redundancy [4]. New encryption techniques have been proposed for encryption of biometric data, chaotic theory has attracted the most due to its properties like sensitivity to initial conditions, ergodicity and their complex behaviour which is difficult to predict and analyse [5]. Chaotic algorithms are divided into two phases scrambling and substitution. In scrambling phase pixels positions are scrambled which results into a scrambled biometric data but scrambling only

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 5, May 2017

will not be an effective solution as it is not resistant against statistical attacks because scrambling effect generates the same histogram of original and scrambled image. Thereby in order to improve the security both phases are combined so that good encryption effect can also be seen. The main contribution of the paper a computationally fast and secure encryption method where strategically diffusion is introduced after scrambling to make the encryption process non invertible to secure the iris biometric data. Compared to conventional encryption schemes, block wise diffusion is done with 3-D Chen chaotic map to change the numerical properties of original biometric data by spreading the effect of each bit of original biometric data completely over encrypted biometric data. Final stage in the fingerprint authentication system is the matching module which decides whether the fingerprint query is either accepted or rejected. The decision is taken by comparing the fingerprint template, which has been stored in the database, with the fingerprint query being processed. Matching can be performed effectively if the fingerprint template and query images largely overlap so that a large number of features can be extracted and compared maximally from those two images using minutiae algorithm.

Paper is organized as follows. Section II includes the basic overview, including the background and motivation. Section III describes the proposed method. The chaotic encryption and the hiding of encrypted image into the captured image are given in Section IV. Section V presents experimental results showing results of images tested. Finally, Section VI presents conclusion.

II. RELATED WORK

Symmetric encryption is faster, thus in contemporary systems a key of size 2^n bits is produced and it is exchanged between the communicating entities, using public key cryptography. However,even though large keys are considered to be safe, it has been proven that any cipher with the perfect secrecy property must use keys with effectively the same requirements as one-time pad keys.The simplest way to encrypt an image or a video is perhaps to consider the 2-D and 3-D stream as a 1-D datastream[2], [4], and then encrypt this 1-D stream with any available key , such a simple idea of encryption is called naive encryption. Although naive encryption is sufficient to protect digital images and videos in some civil applications, this issues have taken into consideration when advanced encryption algorithms are specially designed for sensitive digital images and videos, for their special features arevery different fromtexts. The recent research activities in the field of non-linear dynamics and especially on systems with complex (chaotic) behaviours have forced many investigations on possible applications of such systems. In our case, biometric identifiers are encrypted by a chaotic cipher, which works like a onetime pad in terms of key-size, since the generated key has size equal to the size of the data to be encrypted. Chaotic systems are good for such kinds of tasks, since they present an infinite number of unstable or bits, thus an infinite number of different values. Evolution of the chaotic cipher depends on its initial conditions and the encrypted values of the biometric identiers and thus only the initial conditions should be exchanged between the communicating entities.

Chaos theory[2] describes the behaviour of certain nonlinear dynamic system that under specific conditions exhibit dynamics that are sensitive to initial conditions. The two basic properties of chaotic systems are the sensitivity to initial conditions and Mixing Property. Chaotic map is used to produce the chaotic sequence and used to control the encryption process. The chaos streams are generated by using various chaotic maps. Among the various maps, four maps are investigated and their characteristics are analyzed. A simple and well-studied example of a 1-D map that exhibits complicated behavior is the logistic map from the interval [0,1] in to[0,1], parameterised by μ .The state evolution is described by:

$$g_\mu(x) = \mu * x$$
$$x(n+1) = \mu * x(n) * (1 - x(n))$$

where $0 \leq \mu \leq 4$. This map constitutes a discrete-time dynamical system in the sense that the map $g_\mu : [0,1] \rightarrow [0,1]$ generates a semi-group through the operation of composition of functions. In the logistic map, as μ is varied from 0 to 4, a period doubling bifurcation occurs.

The chaotic encryption algorithm belongs to the category of the combination of value transformation and position permutation. In this method, two different types of scanning methods are used and their performances are analyzed.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 5, May 2017

First, a pair of sub keys is given by using chaotic logistic maps. Second, the image is encrypted using logistic map sub key and in its transformation leads to diffusion process. Third, sub-keys are generated by four different chaotic maps and images are treated as a 1D array by performing Raster scanning and Zigzag scanning. The scanned arrays are divided into various sub blocks. Then for each sub block, position permutation and value transformation are performed to produce the encrypted image. The sub keys are generated by applying the suitable chaotic map banks. Based on the initial conditions, the generated chaotic map banks are allowed to hop through various orbits of chaotic maps. The hopping pattern is determined from the output of the previous map. Hence, for each sub block various chaotic mapping patterns are applied which further increases the efficiency of the key to be determined by the brute force attack. In each orbit, a sample point is taken and used as key for a specific block and a condition to choose the particular orbit in a particular map is adopted. Then, based on the chaotic system, binary sequence is generated to control the bit-circulation functions for performing the successive data transformation on the input data.

Finger-print matching[7] approaches can be categorized into three groups: correlation based, minutiae-based (local) and non-minutiae-based (global) matching. Additionally neural network-based matching, which requires a higher number of data training than the others. Correlation-based matching is performed by lying a fingerprint image over the other. Then, by using a correlation filter, the relation between their corresponding pixels is analyzed. Therefore, in this approach, matching is done by directly correlating the images.

The minutiae-based matching approach, also called local matching, has been widely implemented in authentication systems due to its reliability and accuracy. Here, after being extracted from both template and query images and appropriately represented in the specified format, the minutiae points are compared such that the fingerprint template and the fingerprint query have as many as possible matching minutiae pairs. Different from this, non minutia-based matching (global matching) is performed after aligning the global features. A minutiae point can be represented as a triplet, which consists of its relative position to the core point. Suppose T, m_i and n are the fingerprint template, the minutiae point i^{th} and the total number of minutiae points, respectively; (x_i,y_i) and α_i are the coordinate (i.e.,abscissa,ordinate) and orientation of the minutiae mi with respect to those of corepoint respectively. In this case, the corepoint is the center of the coordinate space and its orientation is aligned with x-axis. The template of a fingerprint can be denoted as:

$$m_i = (x_i,y_i,\alpha_i)$$
$$T = m_i$$

where $1 \leq i \leq n$, (x_i,y_i) € R and $0 \leq \alpha_i < 360^0$. By implementing the similar concepts of those global feature-based representations, local features may be superior due to their stability and reliability. Hence local feature based representation can be constructed by assigning each minutiae point m_i a descriptor, which contains information of its k-nearest neighboring minutiae points.

III. PROPOSED METHOD

The proposed remote human authentication scheme over wireless channels under loss tolerant transmission protocols, aims to ensure: (a) robustness against deciphering, noise and compression, (b) good encryption capacity, and (c) ease of implementation. For this purpose we: (a) employ wavelet-based steganography,(b) encrypt biometric signals to allow for natural authentication, (c) involve a Chaotic Pseudo-Random Bit Generator (C-PRBG) to create the keys that trigger the whole encryption to increase security, and (d) the encrypted biometric signal is hidden in a VO, which can reliably be detected in modern applications that involve teleconferencing. The overall working of the proposed scheme is illustrated in Figure 1. Initially the biometric signal is encrypted by incorporating a chaotic pseudorandom bit generator and a chaos-driven cipher, based on mixed feedback and time variant S-boxes.

Afterwards, a face image of the biometric signal's owner is analysed and the host VO is automatically extracted. Next a DWT-based algorithm is proposed for hiding the encrypted biometric signal to the host VO. The proposed algorithm hides the encrypted information into the largest-value QSWTs of energy-efficient pairs of sub bands. Initially the extracted host object is decomposed into two levels by the separable 2-D wavelet transform, providing three pairs of sub bands (HL_2, HL_1), (LH_2, LH_1) and (HH_2, HH_1). Afterwards, the pair of sub bands with the highest energy content

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 5, May 2017

is detected and a QSWTs approach is incorporated in order to select the coefficients where the encrypted biometric signal should be casted. Finally, the signal is redundantly embedded to both sub bands of the selected pair, using a non-linear energy adaptable insertion procedure. Differences between the original and the stego-object are imperceptible to the human visual system, while biometric signals can be retrieved even under compression and transmission losses.

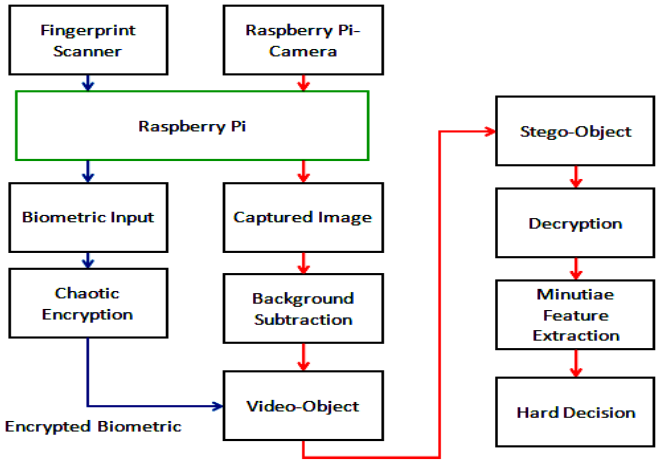

Figure 1. Proposed Block Diagram

IV. CHAOTIC ENCRYPTION AND HIDING TECHNIQUE

The generated key has size equal to the size of each biometric signal. Each key is generated by a C-PRBG. C-PRBGs that are based on a single chaotic system can be insecure, since the produced pseudorandom sequence may expose some information about the employed chaotic system. For this reason, we propose a PRBG based on a triplet of chaotic systems, which can provide higher security than other C-PRBGs. The basic idea of the C-PRBG is to generate pseudo-random bits by mixing three different and asymptotically independent chaotic orbits. Towards this direction let $F_1(x_1,p_1)$, $F_2(x_2,p_2)$ and $F_3(x_3,p_3)$ be three different 1-D chaotic maps:

$$x_1(i+1) = F_1(x_1(i),p_1)$$
$$x_2(i+1) = F_2(x_2(i), p_2)$$
$$x_3(i+1) = F_3(x_3(i), p_3)$$

where p_1, p_2 and p_3 are control parameters, $x_1(0)$, $x_2(0)$ and $x_3(0)$ are initial conditions and $x_1(i)$, $x_2(i)$, $x_3(i)$ denote the three chaotic orbits. Then a pseudo-random bit sequence can be denoted as:

$$k(i) = 1;\ F_3(x_1(i), p_3) > F_3(x_2(i), p_3)$$
$$k(i) = k(i\text{-}1);\ F_3(x_1(i), p_3) = F_3(x_2(i), p_3)$$
$$k(i) = 0;\ F_3(x_1(i), p_3) < F_3(x_2(i), p_3)$$

The operation of the cipher module in Figure.2 can be described as follows: assume that P_i and C_i represent the i^{-th} plain text and i^{-th} cipher text samples respectively (both in n-bit formats). Then the encryption procedure is denoted by:$C_i = f_S(f_S(P_i; i) \| x_i; i)$, where symbol $\|$ represents the xor function, $f_S(i)$ are time-variant n x n S-boxes (bijections denoted on $0,1,...,2^n\text{-}1$) and x_i is produced from the states of three chaotic functions through the bit generation procedure denoted in Equation. Here, the S-boxes f_S are also pseudo randomly controlled by the chaotic functions. The

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 5, May 2017

secret key provides the initial conditions and control parameters of the employed chaotic systems. The increased complexity of the proposed cipher against possible attacks is due to the mixed feedback (internal and external): $f_S(P_i,i)$ at FB_1, $f_S(P_i,i)\| x_i$ at FB_2 and cipher text feedback C_i at FB_3,which lead the cipher to a cyclic behaviour.

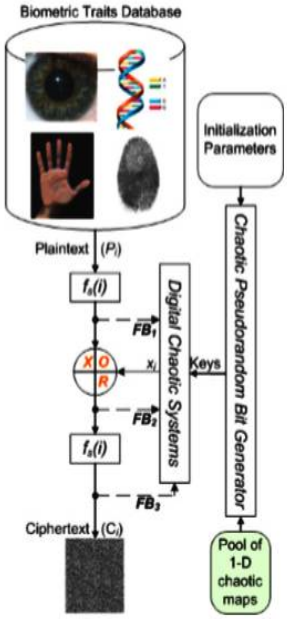

Figure.2 Chaotic Encryption Scheme

The operation of the cipher module in Figure.2 can be described as follows: assume that P_i and C_i represent the i^{-th} plain text and i^{-th} cipher text samples respectively (both in n-bit formats). Then the encryption procedure is denoted by:$C_i = f_S(f_S(P_i; i) \| x_i; i)$, where symbol $\|$ represents the xor function, $f_S(i)$ are time-variant n x n S-boxes (bijections denoted on $0,1,...,2^n-1$) and x_i is produced from the states of three chaotic functions through the bit generation procedure denoted in Equation. Here, the S-boxes f_S are also pseudo randomly controlled by the chaotic functions. The secret key provides the initial conditions and control parameters of the employed chaotic systems. The increased complexity of the proposed cipher against possible attacks is due to the mixed feedback (internal and external): $f_S(P_i,i)$ at FB_1, $f_S(P_i,i)\| x_i$ at FB_2 and cipher text feedback C_i at FB_3,which lead the cipher to a cyclic behaviour. After unsupervised video object extraction is accomplished, each video object is decomposed into three levels with ten sub bands, using the SA-DWT. In the following, the embedment image, which is a visually recognizable pattern, is redundantly embedded to the host video object, by modifying the QSWT coefficients of one of its sub band pairs. In particular, for each video object three pairs of sub bands are examined (since the decomposition is performed into three levels) for possible embedment casting; pair P_1 consisting of subbands (HL_3, HL_2), pair P_2 of sub bands (LH_3, LH_2) and finally pair P_3 of (HH_3, HH_2). The pair of the highest energy content compared to the other two pairs is selected as the most appropriate for embedment casting.

Let us denote as E_{Pk} the energy of P_k, k=1,2,3, which is defined as the sum of the squares of "In-Node" wavelet coefficients of the respective pair of sub bands P_k.

$$E_{pk}=\sum i \sum j \, [x3(i,j)]^2 + \sum p \sum k \, [x3(p,k)]^2 \; ; k=1,2,3$$

where $x3(i,j)$ is an "In-Node" wavelet coefficient of the respective sub band, $x3(i,j) \in Rk$, k=1,2,3, with $R_1=HL_3$, $R_2=LH_3$ and $R_3=HH_3$. Similarly, $x_2(p,q) \in Sk$, k=1,2,3, with $S_1=HL_2$, $S_2=LH_2$ and $S_3=HH_2$. Then the most appropriate pair for embedment casting is selected as the one that maximizes the energy.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 5, May 2017

V. EXPERIMENTAL RESULTS

For evaluation purposes, the proposed video-objects oriented biometric signals hiding scheme is examined interms of security, effectiveness, robustness and bandwidth usage efficiency. The authentication setting, which focused on fingerprints, was simulation based. The general methodology included: extraction of the host video-object from a video conference frame and detection of the QSWTs to embed the encrypted signal, encryption of the fingerprint, embedding of the encrypted signal to the host video object, compression of the final content and simulated noisy transmission, decompression and extraction of the encrypted signal, decryption and authentication.

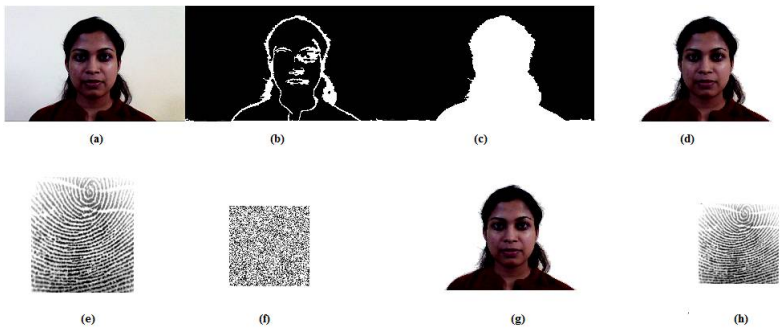

Figure 3. Simulation Results

Figure. 3 shows the simulation results where, (a) represents Input frame, (b) Image after edge detection, (c) Masked image, (d) Background subtraction, (e) Biometric input, (f) Encrypted Biometric, (g) Stego-object and (h) Decrypted Biometric signal respectively. Fingerprint template standards all provide the feature of minutiae quality. The qualities of minutiae have been proved to be good assistant features for improving robustness. For minutiae within overlapping regions, the mean and the variance of their qualities both reveal the reliabilities of the matching results, thus they are all essential information in the global matching stage.

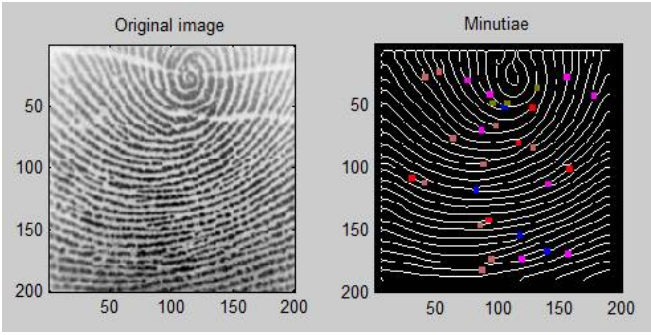

Figure 4. Minutiae features extracted from biometric input.

Figure. 4 represents the minutiae features extracted from the biometric input. Here 100 x 100 biometric image is used. Maximum 25 lines are evaluated from an image and 81 features can be extracted. After training of all databases, minutiae extraction of any image can be evaluated. For testing, we can give any fingerprint to check. If the classified user is accessed, it will shown as recognized otherwise non-recognized.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 5, May 2017

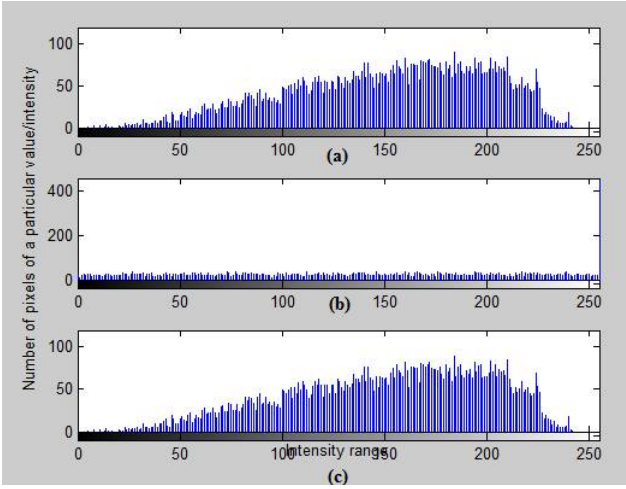

Figure 5. Histogram Comparison

Figure. 5 shows the histogram comparison where, (a) represents Histogram of biometric input, (b) Histogram of encrypted biometric input and (c) Histogram of decrypted biometric signal respectively. The histogram generated for the original image is significantly different from the encrypted image, as it is uniform in nature while that for original image is non uniform. Since the histogram becomes uniform after encryption, the probable chances of predicting similarity between original and ciphered image are nullified.

Algorithm	PSNR of decrypted signal (dB)	PSNR of encrypted signal (dB)
AES	60.4979	11.0713
RSA	67.8420	9.8945
Chaotic Encryption	79.5661	8.3354

Table 1. PSNR Comparison

Table 1 tabulates the PSNR values obtained for the available algorithm and the obtained values verify the explanation. The PSNR is measured to ensure whether the encrypted image is intelligible to unauthorized person or not. The threshold value for PSNR is 79.5661 dB, which means that when PSNR is calculated, and the obtained value is below 28dB that data is intelligible to the unauthorized user else data confidentiality is lost and become easily accessible and usable.

VI. CONCLUSION

As steganography by itself does not ensure secrecy, it was combined with a chaotic encryption system. The proposed procedure, except of providing results that is imperceptible to the human visual system, it also outputs a stego-object that can resist different signal distortions, and steganalytic attacks. Experimental evaluation and detailed theoretical security analysis illustrate the performance of the proposed system in terms of security and randomness. The histogram tests were applied to the encrypted biometric signals (fingerprints in our case) to verify the robustness of the proposed chaotic encryption scheme. Results indicate that the use of QSWTs provides high levels of robustness,

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 5, May 2017

keeping at the same time the ease of implementation and the compatibility to and widely used image. Also, the system is able to recover the hidden encrypted biometric signal.

REFERENCES

[1] Anjal A. Shejul and U. L Kulkarni, "A DWT based Approach for Steganography Using Biometrics Recognition", International Conference on Data Storage and Data Engineering, pages 39-43, June 2010.
[2] Garima Mehta and Malay Kishore Dutta, "Biometric Data Encryption using 3-D Chaotic System", IEEE 2nd International Conference on Communication Control and Intelligent Systems (CCIS), pages 120-140, June 2012.
[3] Ruben Tolosana, Ruben Vera-Rodriguez, Javier Ortega-Garcia, and Julian Fierrez, "Preprocessing and Feature Selection for Improved Sensor Interoperability in Online Biometric Signature Verification cryptosystem", J. Super comput., vol. 63, no. 1, pp. 235-255, May 20, 2015.
[4] Minal Chauhan and Rashmin Prajapati, "Image Encryption Using Chaotic Based Artificial Neural Network" in Proc. ,International Journal of Scientific & Engineering Research, Volume 5, Issue 6, June-2014.
[5] Cai Li and Jiankun Hu, "A Security-Enhanced Alignment-Free Fuzzy Vault-Based Fingerprint Cryptosystem Using Pair-Polar Minutiae Structure",IEEE Transactions on Information Forensics and Security, Vol. 11, No. 3, March 2016.
[6] T. Ahmad and F. Han., "Cartesian and polar transformation-based cancelable fingerprint template", In The 37th Annual Conference of the IEEE Industrial Electronics Society, pages 373-378, 2011.
[7] T. Ahmad, J. Hu, and S. Wang, "Pair-polar coordinate based cancelable fingerprint templates, Pattern Recognition", Volume 44, Issue 10-11, Pages 2555-2564, 2011.
[8] T. Ahmad, J. Hu, and S. Wang. "String-based cancelable fingerprint templates", In The 6th IEEE Conference on Industrial Electronics and Applications, pages 1028-1033 , 2011.
[9] D. Ahn, S. G. Kong, Y, S. Chung, and K. Y. Moon. "Matching with secure fingerprint templates using non-invertible transforms", In The 6th IEEE Conference on Industrial Electronics and Applications, pages 10281033, In Congress on Image and Signal Processing, pages 29-33, 2008.
[10] Sha Wang, Dong Zheng, Jiying Zhao, WaJames Tam and Filippo Speranza, "An Image Quality Evaluation Method Based on Digital Watermarking", Transactions Letters IEEE Transactions on Circuits And Systems For Video Technology, Vol. 17, No. 1, 2007.