International Journal Of
Recent Scientific Research
ISSN: 0976-3031
Volume: 7(4) April -2016

WIRELESS DATA AUTHENTICATION USING SECURE FORCE ALGORITHM

Manimara Boopathy M., Gayathri G., Premalatha S
and Kalpana M

THE OFFICIAL PUBLICATION OF
INTERNATIONAL JOURNAL OF RECENT SCIENTIFIC RESEARCH (IJRSR)
http://www.recentscientific.com/ recentscientific@gmail.com

Available Online at http://www.recentscientific.com

ISSN: 0976-3031

International Journal of Recent Scientific Research
Vol. 7, Issue, 4, pp. 9880-9887, April, 2016

International Journal of Recent Scientific Research

Research Article

WIRELESS DATA AUTHENTICATION USING SECURE FORCE ALGORITHM

Manimara Boopathy M., Gayathri G., Premalatha S and Kalpana M

ECE Department, VELTECH

ARTICLE INFO

Article History:

Received 05th January, 2015
Received in revised form 08th February, 2016
Accepted 10th March, 2016
Published online 28st April, 2016

Keywords:

QSWT, biometrics hiding, remote authentication and steganographic system.

ABSTRACT

In wireless communications, authentication and secure transmission is the need of the hour especially in bank and military communication .The encryption and hiding of image data has been common these days .To improve the security of image transmission to an advanced level, we proposed the concept of secure -force algorithm at the encryption level .Consider the user wanting to send a biometric image being hidden in a image. The image thus obtained is subjected to secure force algorithm, after the encryption to provide invisibility and resistance against lossy transmission. The signal is inserted into QSWT followed by IDWT. Experimental results:(a) increase security (b) bandwidth efficiency (c) hacking would be difficult for the attackers.

INTRODUCTION

In order to confirm the identity of a person or a software program authentication is done. Authentication is the act confirming the truth of an attribute of a datum or entity. Like all other communication networks wireless networks are also prone to security issues. In case remote examinations Trojan horse and other attacks can cause serious problem. Biometric based human authentication over wireless channel under fault-tolerant protocols. There are two types of authentication positive and negative authentication. Positive authentication is applied by the majority of existing authentication. To reduce the cyber-attacks negative authentication is invented. Now a days the method of using passwords for a debit cards and banking transaction is common. This method has become less secure since attackers can easily crack the password. In modern days the password system is being replaced by data hiding encryption scheme. Many algorithms are being implemented but they result in less efficiency. In particular, cryptographic algorithms can scramble biometric signals so that they cannot be understood, while steganographic methods can hide the encrypted biometric signal so that they cannot be seen.

Private Key bulk encryption algorithms such as triple-Des or Blowfish, similar to chaotic algorithms, are more suitable for transmission of large amounts of data. The proposed paper suggests the implementation of secure force algorithm an advanced method of encryption when compared to chaotic encryption. In chaotic encryption, the encryption can be easily cracked by the attackers. Passwords of all the users are authorized to access are stored, usually in files. Password space includes only user's passwords and it is limited. If the hackers receives the password, their work is to recover the plaintext of very limited number of password. On the contrary, in negative authentications if the anti-password space is created, containing all the strings are not in that passwords file. If hackers receives the large anti-password file, their work will be a much harder than other. In this way, the negative authentication can be introduced a new layer of protect into enhance existing security measures within the networks. It allows the current infrastructure to remain the intact without accessing a stored passwords. Applying a real-valued algorithm, a different layer is added in authentication, preventing the unauthorized from gaining networked access. The Interested readers can also be check.

If the proposed scheme is a positive authentication and for the security reasons elements, and preferably of the following factors should be verify: • the ownership factor: the user as (e.g. ID card, security token, cell phone etc.) • the knowledge factor: if the user knows (e.g., a password, a PIN, a pattern etc.) • the inherence factor: if the user is or does (e.g., fingerprint, retinal pattern, DNA sequence, face, other biometric identifier etc.) In 2012 identifying the fraud in US they affected 12.6 million consumers, and resulted in a loss of $3.6 billion

**Corresponding author: Manimara Boopathy M*
ECE Department, VELTECH

($365/consumers). Probability of becoming a fraud victim is approximately 5.2%. As a result, robust remote the human authentication becomes the most of the important issues contemporarya societies and workers of several have been proposed in a literature it is effectively tackle it. The majority is fully based on passwords or smart cards. In Section II-A, the pros and cons of the systems are explained and the use of biometrics is suggested as an alternative method. Biometrics have already incorporated in a remote authentication (see [3], [4], [5]) but only a password substitution in a smart cards. In order to investigate their potential fully, if the biometrics can incorporated in hybrid steganography schemes.

In particular, if the cryptographic algorithms can be scramble the biometric signals. So they cannot be understood, while stegano methods can be hide the encrypted biometric signal, so that could not be seen. In this paper, we further build on this principle to confront of the problem of remote human authentication over wireless networks, under loss tolerant protocols. In particular effective wavelet-based method is proposed for a hiding an encrypted signals semantically meaningful Video object such as the head-and-shoulders, which is used common in several teleconferencing applications. The rest of this paper is described as follows: Section II focuses on the contributions and innovations of the proposed scheme. In Section III a high level description of the proposed system is presented along with justification in theoretical Description of the chaotic encryption method in Section IV while Section V focuses on the insertion of the encrypted image into the host video object. Section VI includes experimental results while Section VIII concludes this paper.

Related Work and Contribution

In a Remote Authentication, Lamport [6] proposed a remote password authentication scheme. However, in this scheme a verification table should be and if intruders break into it, if they can modified the fixed table. Therefore, many of the different solutions have been proposed early, the most popular which is based on the long and the random cryptographic methods [7]. For this instance, Liao *et al*. [8] proposed a scheme that utilized a Diffie-Hellman key agreement protocol over the insecure networks, which allows the particular user and the system to be agreed on a session key to encrypt or decrypt in their communicated messages using a symmetric system. Random cryptographic keys are very difficult to memorized, if they are stored somewhere and they released based on the some alternative authentication mechanism like password. However the several passwords are simple and they can be easily guessed [9] by others, [10]. Furthermore, most people use the same password in a different applications; if the malicious user find a single password, they can access by multiple applications.

Another very interesting and a promising category of remote authentication schemes involves smart cards by using the dynamic users. If the identities per transaction section [11], [12], [13]. These methods are used to overcome a common drawback of the older remote authentication scheme is using smart cards: user's identity was static in all the transaction sessions, which may be leak some information about that particular user and can be create a risk of ID-theft ,the message transmission over an insecure channel. However, the vulnerabilities of these methods are also found. Madhusudhan and Mittal [14] proposed a security requirements and goals for remote user password authentication schemes, and through the respective cryptanalysis, proved that both Wang's *et al*. [11] and Khan's *et al*. schemes [12] were insecure against the insider attacks while where the password authentication is delayed and inefficient. Weaknesses of Yoon's *et al*. [13] method were also reported (see [15]). Some of the latest schemes, such as [16], [17] seem very interesting. Still the virtues are should be thoroughly is investigated by applying a cryptanalysis, differential power analysis, physical disassembly Additionally: (a) users should always have the smart cards with them in order to do any transactions, (b) if the users loses his or her smart card, he or she will not be able to do the transactions and should wait for reissuing of the smart card , (c) smart cards have cost money and they effort each time they are issued or reissued, (d) due to low power they cannot be performed very complex computations, (e) according to the cardwerk.com their memory should be retain the data for up to 11 years without electrical power and (f) they should be support at least 10,000 read-write actions during the life of the smart cards. Many of the password based authentication problems can be confronted by using biometrics [18]. Biometrics are inherently reliable, since the biometric traits are cannot be lost ,then they are more difficult to forge, copy, and distribute and they did not require any person being authenticated to be present at that time and the point of authentica-tion[19], [20]. Recently, the biometrics signal have been extensively applied in remote authentication and several methods were reported [3], [4], [5], [21]. In this majority of these schemes ([3], [4], [5]) biometrics are used simply as a authentication tool in card technology. The drawbacks mentioned in the previous paragraph still hold. Furthermore, as reported in [21] they cannot provide and three-factor security while they are vulnerable to the privileged to be inside and the user of impersonation attacks.

B. Steganographic methods…S Algorithms can be roughly divided in spatial domain and those applied in that transform domain they are more robust against low-pass filter and their compression attacks [22], if they will became an approach. Among the transform-based hiding DCT and DWT methods, they are most popular since they are related with the popular digital image and the video compression schemes H2. if the message is hidden in the signed values of insignificant children of the subbands, Using this technique, the steganographic messages can be send in the lossy environments, with some robustness against detection the attack. However, the low level losses are considered and problem of the remain compressions. this message is compressed of two components: a soft-authenticator watermark authentication, the tamper assessment, the chrominance watermark employed used to improve the efficiency of the compression. This approach should be implemented as a DCT-DWT dual domain, but the authenticator watermark is not encrypted. The similar approaches for combining DWT and Integer Wavelet Transform (IWT) was proposed by Hemalatha *et al*. where both of that secret images and the key are encrypted in the cover images. However, the embedding algorithm is complex and their sensitive to that lossy transmissions. There also some schemes for that focusing on the steganographic of the biometric signals .The amplitude modulation- based scheme was proposed, however is not tested under that compression. In a wavelet-based steganographic method for embedding has been proposed. Nevertheless if our opponents know that embedding algorithm, they can easily extracted the hidden information from the original image. The fingerprints are hidden in the region of the images. Both of the DFT and DWT domains are examined. However, no encryption is in corporated. Another method, but not resistant, the method is proposed in where a remote biometrics authentication framework should be works on the basis of fragile watermarking. Finally a DCT-SVD based watermarking scheme is proposed for the individual protection. The scheme is not tested under compression or transmission. The last category of approaches involves hiding the data within an image or the video objects over the cover image. Object- oriented hiding of data is secured and more robust against the attacks but it is usually creates the sensitive artifacts, thus the capacity of encryption. Furthermore, the detection of objects in both the images and videos by no-means. As the result the majority of methods in this category hiding of data either in the skin areas of the cover images or in the areas of simplicity defined through the extraction ofa specific descriptors. The Detection of skin like color and feature descriptors are robust but rarely lead to the large of compact objects, reduced the further more encryption capacity.

Contribution of the current work

In contrast to the existing methods mentioned in that previous sections, if the main contributions are analyzed: 1) Biometrics-based human authentication over wireless channels: The overriding majority of their current works does not consider the tolerant protocols if the transmission of the stegoobjects. With that the proposed approach of several mobile applications could be benefitted. For example in an emerging, let us imagine that the users would be like to authenticated. If her mobile device has a camera, while its touch screen collaborates with a fingerprints capturing applications. In case that the strength of the signal is low, enormous packets may be arrived at the receiver. Thus the scheme like the proposed is required. 2) Automatic extraction of semantical, the meaningful video objects for embedding, their encrypted biometric information. Most of the existing schemes did not consider the semantically meaningful VOs as a hosts, but in a whole image. If the proposed scheme offers some possible advantages. Firstly, the schemes should be provides a secondary complementary authentication mechanism. if in case when the person under the authentication is also captured by a camera. Thus her face and body is transmitted together with a another biometric feature for the possible double authentication. Secondly, in a every recent transaction, the overall architecture can be stored at the latest sample pictures of ones face and body. This could be help in cases of hybrid authentication, when both the machines and the human remotely authenticated a person. This machine can be authenticated the fingerprint and the human can authenticate the face. Another advantages to do with more usage of efficient bandwidth, especially in their abovementioned in the case of hybrid remote authentication. An image is usually did not contained a semantically meaningful information but also the background blocks. On the other hand, in order to do hide a specific amount of information, a host with the proper capacity should be selected. If the host is an image that irrelevant blocks will be transmitted, occupying a valuable bandwidth. On that contrary, when their host is a semantic Video Object, all the transmitted information is relevant to the authentication. The proposed scheme allows for more efficient than rate control and can be better confront the traffic congestions. For example, in a steganographic algorithm which uses the images, and if the traffic congestion occurs, all the image blocks would be probably considered an equal importance. On the other hand, the proposed scheme is a content aware. In case of the traffic congestion, then the rate control of mechanism could be discard all the blocks from the body region that do not also contained the hidden information, instead of discarding the face areas. 3) Chaotic cipher, which works like a one-time pad, to encrypt the biometric identifiers: Symmetrical encryption is more faster, thus the contemporary systems a key of size 2n bits is produced and it is exchanged between the communicating entities, used a public key cryptography. However, an even though a large keys are considered to be safe, it has been proved that the cipher with the perfect secrecy must use the keys with the effectively same requirements as one time pad keys [40]. In a case, the biometric identifiers are encrypted by a chaotic cipher, which should be works like a one-time pad in terms of key-sized, since they will generated the key has equal size to the data size to be encrypted. Chaotic systems are good for such kinds of the tasks, since they will present an infinite number of an unstable orbits, thus an infinite number of different values. Evolution of the chaotic ciphers on its initial conditions and the encrypted values of a biometric identifiers and thus only the initial conditions should be exchanged between the communication. In this proposed scheme the exchange is also performed by the incorporating public key cryptography.

The Existing Method

The existing remote human authentication scheme was over the wireless channel sunder the loss tolerant transmission protocols, aims to ensure: (a) robustness against deciphering (b) good encryption capacities (c) ease of implementation. For this purpose we: (a) employ the wavelet-based steganography, (b) The encrypted biometric signals to allow for the natural authentications,(c)involve the Chaotic Pseudo-Random Bit generator(C-PRBG)to create that keys they trigger of the whole encryption to increase the security, and (d)the encrypted biometric signal is hidden, which can reliably be detected in the modern applications that involved at conferencing. The overall architecture and data flow of the existing schemeis illustrated. Initially the biometric signal is encrypted by incorporating a chaotic pseudo-random bit generator and a chaos-driven cipher, based on the mixed feedback and time variant S-boxes. The uses of such an encryption mechanism is justified

1) chaos presents sensitivity to initiated the conditions
2) C-PRBG statistically works very well as a one-time pad generator,
3) The implementation of a popular key encryption methods, such as RSA or El Gamal, cannot be provided a suitable encryption rates. This is almost all of the temporary encryption algorithms

Combine the symmetric and public key cryptography. The security of these algorithms in theory, the difficulty of the quickly factorizing large number for solving a discrete logarithm and, in practice, on the difficulty of recording acoustic emanations. However both the levels (theoretical and practical) may be challenged by are advances in the number theory, the distributed computing and the acoustic cryptanalysis. In particular on December12, 2009, Kleinjung *et al*. it have factored the 768-bit, 232-digitnumberRSA-768by the number field. The number RSA-768wastaken from the RSA Challenge list[1].The authors is claimed it is not a unreasonable expect that the 1024- bit modulation can very well precisely because susceptible being broken.2048 bit RSA, in comparison, is approved until 2003 and disallowed there after. Of course that a for mentioned references mean that if someone has recorded our encrypted communication with its 1024-bit RSA and factorization of1024-bitis accomplished with in this decade, then the data from the past. On the other hand, regarding the acoustic cryptanalysis, Genkin *et al*. numbers acoustic cryptanalyst is key extraction attacks, applicable to the Gnu PGs current implementation of RSA. The attack can be extract full 4096-bit RSA decryption keys from laptop computers (of various models), with in an hour, using that sound generated by the computer during the decryption of some chosen ciphertexts. They experimentally demonstrate that such attacks can be carried out, using either a plain mobile phone placed next to the computer, or a more sensitive microphone placed four meters away,

4) private-key bulk encryption algorithms such as Triple-DES or Blowfish, similarly to chaotic algorithms, are more suitable for transmission of large amounts of data. Are considered secure enough when implemented correctly, however, due to the complexity of their internal structure, they cannot be concisely and clearly explained, so that to enable detection of possible cryptanalytic vulnerabilities, if any. In particular, faulty implementations may make both algorithms in secure (e.g. meet-in-the-middle attack for Triple-DES[44] or reflectively weak keys attack for Blowfish [45]).Furthermore the FAQ for Gnu PG[2] recommends that Blowfish should not be used to encrypt files that are larger than 4Gb.

Ahead-and-body image of the biometric signal's owner is analyzed and the host VO is automatically extracted based on the method existing in [46].Next a DWT-based algorithm is existing for hiding the encrypted biometric signal to the host VO. The existing algorithm hides the encrypted

Information into the largest-value QSWT of energy-efficient pairs of sub bands. In corporate approach has the following advantages [47];

- it is one of the most efficient algorithms of literature that has facilitates robust hiding of visually recognizable patterns
- it is hierarchical and has multire solution characteristics, the embedded information is hard to detect by the human visual system (HVS), and
- it is among the best known techniques with regards to survival of hidden information after image compression facilitates robust hiding of visually recognizable patterns,
- the embedded information is hard to detect by the human visual system (HVS).

Initially the extract host object is decomposed into two levels by the separable2-Dwavelet transform, providing three pairs of subbands (HL_2, HL_1), (LH_2, LH_1) and (HH_2, HH_1). Afterwards, the pair of subbands with the highest energy content is detected and a QSWTs approach is incorporated [48] in order to select the coefficients where the encrypted biometric signal should be casted. Finally, the signal is redundantly embedded to both subbands of the selected pair, using a non-linear energy adaptable insertion procedure. Difference between the original and the stego-object are imperceptible to the human visual system (HVS), while biometric signal scan beretrieved even under compression and transmission losses.

Chaotic Encryption

Before hiding, each biometric signal is initially encrypted. Encryption is performed by the existing chaotic crypto- graphic module of Fig.2. The module includes a Chaotic Pseudo-Random Bit Generator(C-PRBG) and a chaos-based cipher mechanism.

Encryption Key's Generation

In most contemporary schemes security of the encrypted content mainly depends on the size of the key .In this paper, 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 in secure, since the produced pseudorandom sequence may expose some information about the employed chaotic system [49]. For this reason in this paper we propose a PRBG based on a triplet of chaotic systems, which can provide higher security than other C-PRBGs [50].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 different1-Dchaoticmaps:

x1(i+1)=F1(x1(i),p1)
x2(i+1)=F2(x2(i),p2)
x3(i+1)=F3(x3(i),p3)

where p_1,p_2 and p_3 are control parameters ,$x_1(0)$, $x_2(0)$and $x_3(0)$are initial conditions an d$x_1(i)$,$x_2(i)$,$x_3(i)$denote the three chaotic orbits.

According to this scheme the generation of each bit is controlled by the orbit of the third chaotic system, having as initial conditions the outputs of the other two chaotic systems

The Encryption Mechanism

After generating the initial pseudo-random key, the cipher module is activated. Before encryption, the samples of each biometric signalareproperlyordered.Incaseof1-Dsignals (e.g. voice) the order is defined by the sequence of samples, while in 2-D signals (e.g. finger print image) pixels are line per line zig-zag scanned from top-left to bottom-right, providing plain text pixels P_i. Next, we take into consideration the fact that multiple iterations of chaotic functions lead to slow ciphers, while a small number of iterations may raise security problems [50].In order to avoid iterations while maintaining high security standards, the existing scheme combines three chaotic block ciphers (including the time variant S-boxes) to implement a complex product cipher. Considering Fig.2 the operation of the cipher module can be described as follows: assume that P_i and C_i represent theirthe plain extanding cipher text samples respectively (both in-bit formats).Then then cryption procedure is defined by:

$$C_i=f_S(f_S(P_i,i)\oplus x_i,i) \text{ ----}\rightarrow \qquad (2)$$

Where symbol ⊕ represents the XOR function, $f_S(\cdot,i)$ are time-variant S-boxes(bijections definedon0,1,,2^n-1)
And x_i is produced from the states of three chaotic functions throughthebitgenerationproceduredefinedineq.1.Here
PRBG. However PRBG's pass the tests of NIST suitable for cryptographic applications.

The first 768 bits produced by C-PRBG feed digital chaotic systems sub module(DCSS).DCSS works in same way as the C-PRBG, but the initial values of p_1, p_2, p_3, $x_1(0)$, $x_2(0)$ and $x_3(0)$ are provided by the C-PRBG(firstset128bitsforp$_1$, second set128bitsforp$_2$ etc.).Role of the DCSS is to cover sequences (~1-2%)produced by the C-PRBG pass all NISTs tests (see Section VI, Table I, third column).In order to resist chosen plain text and cipher text attacks algorithm's behavior continuously changes, based on specific content that to be encrypted .In particular plaintext P_i is cut into chunks of 384 bits. Each chunk

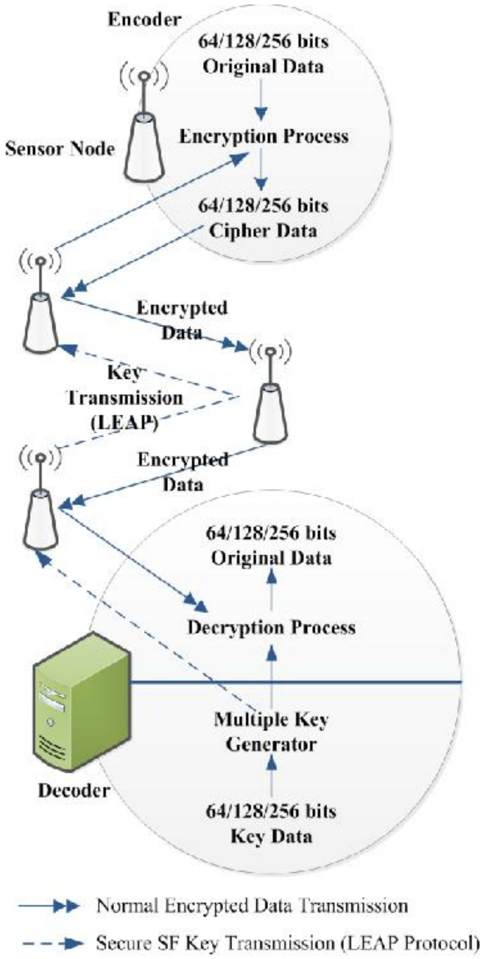
Operation Mode Analysis

The security merits of chaotic encryption are due to the combination off our modes of operation. The mode of operation describes repeatedly apply cipher's single-block operation to securely transform of data larger than block. In particular in Fig.3 modes of operation of the existing encryption module is described.

The existing scheme consists of one Cipher-Block Chaining(CBC) mode of operation (red frame)and three Key Feedback Modes(KFB)operation(green frame).Initial plain text through a block cipher encryption procedure depicted as Block Cipher Encryption-A(the first f_S(i) of shown inFig.2) produce cipher- text C_1.C_1 provides feedback to Block Cipher Encryption-1(Digital Chaotic Systems block Fig.2)and changes the encryption key(KFB-1),producing Block Cipher Encryption-2.Output Block Cipher Encryption-2 is then XOR with C_1,produce C_2.C_2 provides feedback to the Block Cipher Encryption-2(Digital Chaotic Systems shown inFig.2)and changes the encryption key for second time (KFB-2). C_2 passes through the block cipher encryption procedure depicted as Block of Cipher Encryption-B (the second f_S(i) shown inFig.2), producing the output C_3.C_3 provides feedback to Block Cipher Encryption-3(Digital Chaotic Systems block shown in Fig.2)and changes encryption key for third time(KFB-3).A sequence of keys is continuously produced, have size equal to size of the plain text to been encrypted. since, three KFB modes are incorporated so as to toughen up acoustic cryptanalysis attacks. In particular even if a key is revealed, it will not been ought to decrypt the image, since different keys are used in every cycle of the existing scheme. Thus, even in case of acoustic cryptanalysis, the cryptanalyst should record thew hole encryption process and not only the first 1024or2048bits.This condition is also valid even in case the acoustic cryptanalyse that compromised the three secret control parameters p_1,p_2 and p_3 and three secret initial conditions $x_1(0)$, $x_2(0)$ and $x_3(0)$ of the C-PRBG, since the process heavily depends on the provided plaintext

Secure-Force Algorithm

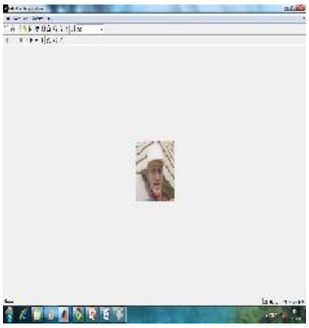
The Secure Force algorithm based on Fiestel architecture. Here process of encryption and decryption are same, resulting in minimization of the code size to the extent. Low-complexity architecture provided by SF algorithm for implementation WSN. The encryption process consists of only five encryption rounds. This helps in improving the energy efficiency. It has been realized that lower the number of encryption rounds lesser the power consumption. Each encryption round encompasses six simple mathematical operations operating on only 4 bit data (designed to be compatible with 8-bit computing devices for WSNs). This creates an adequate amount of confusion and diffusion.

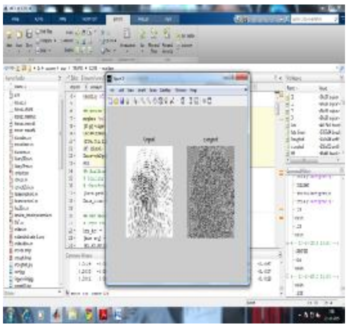


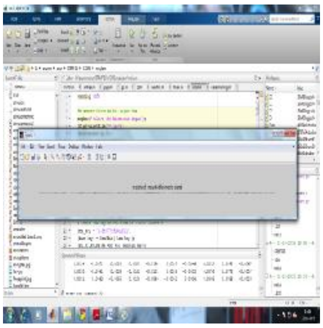
Permutation, transposition and rotation) to generate keys for the encryption process, is implemented at the decoder.

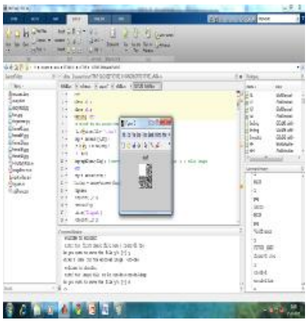
The computational burden to the decoder and indirectly, this will help to increase the lifespan of the sensor nodes. However, the generated keys must be transmitted securely to the encoder for the encryption process. In this case, the LEAP (Localized Encryption and Authentication Protocol) is adopted. It is an energy efficient, robust and secure key management protocol that is designed for the WSN. Overall, the process of SFalgorithm consists of 4 major blocks. The detail description of each block of the Secure Force algorithm can be found in [1].

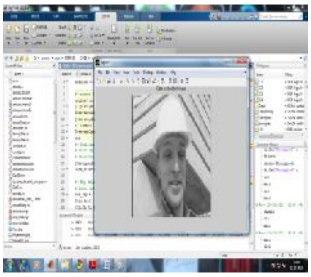
Experimental Evaluation

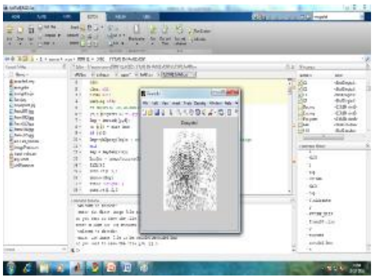












An image is extracted from a video object as shown. The video object shown here is known as the foreman image. In this image, and the encrypted biometric signal is hidden. Any other image can also be used for the purpose of hiding the biometric signal. Before hiding the biometric signal in video object, it is first encrypted using secure force algorithm for ensuring its secure transmission in an enhanced way.

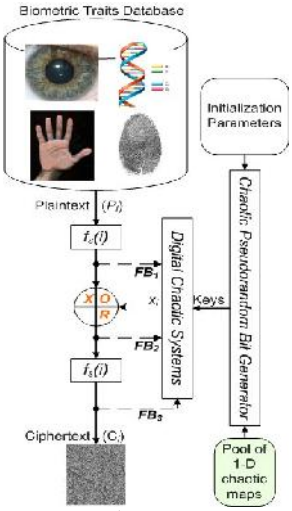
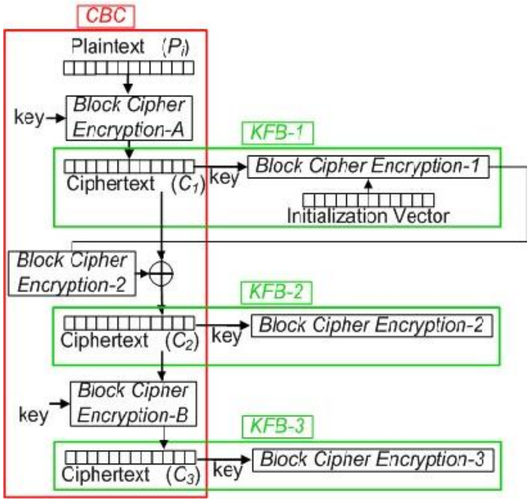


Fig.2 Overview of the Encryption Module

During encryption, the biometric signal gets hidden completely making it difficult for attackers to obtain them. The encrypted image is then vectorized. During this process each pixel in the image is converted into a single row or a single column that can be represented in the matrix form as 1xn or nx1. Vectorisation is done in order to achieve easy compression. After vectorising the signal is transformed using discrete wavelet transform (DWT). By applying DWT to an area of arbitrary shape, four parts of low, middle, high frequency i.e., HL, LH, LL, HH. Here LL sub band is used for efficient compression purpose. bioiometric signals enter more and more into our everyday lives, since governments, as well as other organizations, resort to their use in accomplishing crucial procedures (e.g. citizen authentication).


CBC
Plaintext (P_i)
key
Block Cipher Encryption-A
KFB-1
Ciphertext (C_1)
key
Block Cipher Encryption-1
Initialization Vector
Block Cipher Encryption-2
KFB-2
Ciphertext (C_2)
key
Block Cipher Encryption-2
key
Block Cipher Encryption-B
KFB-3
Ciphertext (C_3)
key
Block Cipher Encryption-3

Thus there is an urgent need to further develop and integrate biometric authentication techniques into practical applications. Towards this direction the domain of biometrics authentication over error-prone networks has been examined .Since steganography by itself does not ensure secrecy, it was combined with a chaotic encryption system. The proposed procedure, which provides 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.

References

1. A. Madero, Password secured systems and negative authentication. Thesis: S.M. in Engineering and Management, Massachusetts Institute of Technology, Engineering Systems Division, 2013. Available: http://hdl.handle.net/1721.1/90691
2. 2013, “Identity fraud report: Data breaches becoming a treasure trove for fraudsters,” Javelin Strategy and Research, Tech. Rep., 2013.
3. E.-J. Yoon and K.-Y .Yoo, “Robust biometrics-based multi-server au- thentication with key agreement scheme for smart cards on elliptic curve cryptosystem,” The Journal of Supercomputing, vol. 63, no. 1, pp. 235–255, Jan. 2013.
4. H. Kim, W. Jeon, K. Lee, Y. Lee, and D. Won, “Cryptanalysis and improvement of a biometrics-based multi-server authentication with key agreement scheme,” in Computational Science and Its Applications, ser. Lecture Notes in Computer Science, vol. 7335. Spinger-Verlag, 2012, pp.
5. M.-C. Chuang and M. C. Chen, “An anonymous multi-server authenti- cated key agreement scheme based on trust computing using smart cards and biometrics,” Expert Systems with Applications, vol. 41, no. 4, pp. 1411–1418, Mar. 2014.
6. L. Lamport, “Password authentication with insecure communication,” Communications of the ACM, vol. 24, no. 11, pp. 770–772, 1981.
7. W. Stallings, Cryptography and Network Security: Principles and Prac- tices. Prentice-Hall, 5th edition, Upper Saddle River, NJ, USA, 2010.
8. I.-E. Liao, C.-C. Lee, and M.-S. Hwang, “A password authentication scheme over insecure networks,” Journal of Computer and System Sciences, vol. 72, pp. 727–740, 2006.
9. M. Jakobsson and M. Dhiman, “The benefits of understanding pass- words,” in Mobile Authentication, ser. SpringerBriefs in Computer Science. Springer New York, 2013, pp. 5–24
10. M. Weir, S. Aggarwal, M. Collins, and H. Stern, “Testing metrics for password creation policies by attacking large sets of revealed passwords,” in Proceedings of the 17th ACM Conference on Computer and Communications Security. ACM, 2010, pp. 162–175.
11. Y.-y. Wang, J.-y. Liu, F.-x. Xiao, and J. Dan, “A more efficient and secure dynamic id-based remote user authentication scheme,” Computer Communications, vol. 32, no. 4, pp. 583–585, Mar. 2009.
12. M. K. Khan, S.-K. Kim, and K. Alghathbar, “Cryptanalysis and security enhancement of a ‘more efficient & secure dynamic id-based remote user authentication scheme’,” Computer Communications, vol. 34, no. 3, pp. 305–309, Mar. 2011.
13. E.-J. Yoon, S.-H. Kim, and K.-Y. Yoo, “Cryptanalysis and security enhancement of a ‘more efficient & secure dynamic id-based remote user authentication scheme’,” *International Journal of Innovative Computing*, Information and Control, vol. 8, no. 5(B), pp. 3661–3675, May 2012.
14. R. Madhusudhan and R. C. Mittal, “Dynamic id-based remote user pass- word authentication schemes using smart cards: A review,” Intelligent Algorithms for Data-Centric Sensor Networks, vol. 35, no. 4, pp. 1235–1248, Jul. 2012.
15. T.-Y. Chen, C.-H. Ling, and M.-S. Hwang, “Weaknesses of the yoon- kim-yoo remote user authentication schemeusing smart cards,” in Proceedings of the 2014 IEEE Workshop on Electronics, Computer and Applications. IEEE, 2014, pp. 771–774.
16. A. K. Das, “A secure and effective user authentication and privacy preserving protocol with smart cards for wireless communications,” Networking Science, vol. 2, no. 1-2, pp. 12–27, May 2013.
17. T.-Y. Chen, C.-C. Lee, M.-S. Hwang, and J.-K. Jan, “Towards secure and efficient user authentication scheme using smart card for multi- server environments,” *The Journal of Supercomputing*, vol. 66, no. 2, pp. 1008–1032, Nov. 2013.
18. A. K. Jain, A. Ross, and S. Prabhakar, “An introduction to biometric recognition,” IEEE Transactions on Circuits Systems for Video Technol- ogy, vol. 14(1), pp. 4–20, 2004.
19. C.-T. Li and M.-S. Hwang, “An efficient biometrics-based remote user authentication scheme using smart cards,” *Journal of Network and Computer Applications*, vol. 33, no. 1, pp. 1–5, Jan. 2010.
20. A. K. Das, “Analysis and improvement on an efficient biometric-based remote user authentication scheme using smart cards,” IET Information Security, vol. 5, no. 3, pp. 145–151, Sep. 2011.
21. D. He and D. Wang, “Robust biometrics-based authentication scheme for multi-server environment,” *IEEE Systems Journal*, pp. 1–8, 2014.
22. M. Ramkumar and A. N. Akansu, “Capacity estimates for data hiding in compressed images,” IEEE Transactions on Image Processing, vol. 10(8), pp. 1252–1263, 2001.
23. N. Provos and P. Honeyman, “Hide and seek: An introduction to steganography,” IEEE Security and Privacy, vol. 1(3), pp. 32–44, 2003.
24. P.-Y. Chen and H.-J. Lin, “A dwt based approach for image steganog- raphy,” *International Journal of Applied Science and Engineering*, vol. 4(3), pp. 275–290, 2006.
25. S. Areepongsa, Y. F. Syed, N. Kaewkamnerd, and K. R. Rao, “Steganog- raphy for a low bit-rate wavelet based image coder,” in Proceedings of the IEEE International Conference on Image Processing, vol. 1. IEEE, 2000, pp. 597–600.
26. D. Kundur, Y. Zhao, and P. Campisi, “A steganographic framework for dual authentication and compression of high resolution imagery,” in Proceedings of the IEEE International Symposium on Circuits and Systems, vol. 2. IEEE, 2004, pp. 1–4.
27. S. Hemalatha, U. Dinesh Acharya, A. Renuka, and P. R. Kamath, “A secure age steganography in transform domain,” *International Journal on Cryptography and Information Security*, vol. 3(1), 2013.

28. J. Dong and T. T., “Security enhancement of biometrics, cryptography and data hiding by their combinations,” in Proceedings of the 5th International Conference on Visual Information Engineering. VIE 2008, 2008, pp. 239–244.
29. A.K.Jain and U.Uludag, “Hiding biometric data,” IEEE Tr Tansactions on Pattern Analysis and Machine Intelligence, vol. 25(1) (11), pp. 1494– 1498, 2003.
30. K. Zebbiche, L. GhouF. Khelifi, and A. Bouridane, “Protecting fin- ger print data using watermarking,” in Proceedings of the 1st NASA/ESA Conference on Adaptive Hardware and Systems. IEEE Computer Society, 2006, pp. 451–456.

****

How to cite this article:

Manimara Boopathy M *et al*.2016, Wireless Data Authentication Using Secure Force Algorithm. *Int J Recent Sci Res.* 7(4), pp. 9880-9887.

ISSN 0976-3031

9 770976 303009 >