Journal of Computer Science 8 (7): 1012-1021, 2012
ISSN 1549-3636

Multimodal Biometric-based Secured Authentication System using Steganography

Shanthini, B. and S. Swamynathan
Department of IST, Anna University, Chennai, India

Abstract: Problem statement: The main challenge in the design of a security system for high security mobile ad OC network is how to prevent the attacks against data modification and authentication. **Approach:** In this novel proposed system the messages communicated between the users are encrypted by the cancellable cryptographic key generated from fingerprint features of the receiver by applying genetic operators and are embedded inside the scrambled face biometrics of the sender using steganography method. **Results:** The receiver first unscrambles the facial image of the sender and separates the facial image and the encrypted data. Then he verifies the sender by using an Eigen face recognition algorithm and if he is a genuine sender he decrypts the cipher text with the key generated using the receiver's fingerprint biometric. **Conclusion/Recommendations:** By this way, the receiver ensures the genuineness of the sender and data confidentiality. Revocability is also guaranteed since we apply genetic operator to randomize the cryptographic key whenever it is necessary. By simulation results, we also show that the proposed method is more efficient mechanism for authentication and security.

Key words: MANET, data security, authentication, multimodal biometrics, steganography, genetic algorithm

INTRODUCTION

Message security plays a crucial role in data transmission in high security applications such as military, healthcare, intelligent building systems. The main challenge in designing a security system for MANET is how to prevent the attacks against data such as unauthorized data alteration, impersonation, interception, fabrication, (Stallings, 2010). The best way to protect the information in a most fine-granular way is by providing security using cryptography. Verifying whether the sender is genuine or not is also equally important in a high security environment such as military scenario (Trivedi *et al*., 2009) where the most strategic, deliberate and tactical information is communicated.

So, in this study, we present a novel security model which provides security and authentication using multimodal biometrics coupled with steganography.

Cancellable multimodal biometrics: Mission-critical applications may have higher requirements regarding information security and user verification. Numerous countermeasures such as strong authentication, encrypting and decrypting the messages using traditional cryptographic algorithms are used to tackle the attacks on MANETs. Even though these traditional approaches play an important role, these are not sufficient for more sensitive applications and also MANETs (Trivedi *et al*., 2009) cannot support complex computations or high communication overhead due to the limited memory, computation power and low battery life of mobile nodes. So, in such a mission-critical scenario, we need to design a security system which combines biometrics, cryptography, authentication and steganography to overcome the limitations of traditional security solutions.

Biometrics (Jain *et al*., 2008) refers to the methods for uniquely recognizing human based upon one or more intrinsic physical or behavioral traits. As biometrics can't be borrowed, stolen, or forgotten and forging is practically impossible, it has been presented as a natural identity tool that offers greater security and convenience than traditional methods of personal recognition such as using passwords. The best biometric that can easily be deployable is a fingerprint recognition (Maltoni, 2003) and face recognition (Li and Jain, 2005) since these biometric have been successfully deployed in many civilian identification for years. Even though biometric has advantages, it also raises many security and privacy concerns like: biometric is authentic but not secret, biometric cannot

Corresponding Author: Shanthini, B., Department of IST, Anna University, Chennai, India

be revoked or cancelled, if a biometric is lost once, it is compromised forever and cross-matching can be used to track individuals without their consent. To overcome these disadvantages, instead of using a single biometric, multimodalbiometrics (Ross *et al*., 2006) which may have the combinations of different biometric like fingerprint, face, teeth, iris, handwriting and voice (Kim and Hong, 2008; Humm *et al*., 2009; Anand *et al*., 2010) or biometrics combined with challenge-response method like password (Chen *et al*., 2012) can be used for the security system.

As multimodal biometric consolidates the information from multiple biometric sources, the effective fusion of information obtained is a challenging task (Komninos *et al*., 2007) and so a multilevel security system is proposed for confidentiality and authentication using cancellable multimodal biometric. Cancellable means the original biometrics is not used as such; instead, a cancellable form of it is used. That is a set of features are extracted from the fingerprint biometrics and then genetic operation is applied to get different keys for different transactions. A two-point crossover operator is used here to randomize the feature set to obtain cryptographic key so that if a biometric is compromised, it can be simply reenrolled using another genetic operation, thus the revocability of the biometric is preserved.

Genetic algorithms and steganography: Genetic algorithms (Fessi *et al*., 2009) are a family of models inspired by natural evolution. They belong to the field of evolutionary computation and are based on three main operators: Selection selects the fittest individuals, called parents that contribute to the reproduction of the population at the next generation, Crossover combines two parents to form children for the next generation and Mutation applies random changes to individual parents to form children. Genetic algorithms are used as an aiding tool for generating and optimizing security protocol (Zarza *et al*., 2007). The security protocols can be represented as binary strings and Genetic Algorithm tools are used to define genome interpretation in optimization problems.

Steganography is an ancient art of hiding messages in a secret way that no one, apart from the sender and anticipated recipient, suspects the existence of the message. The advantage of steganography, over cryptography, is that messages were hidden inside the image in steganography and that do not attract attention of others to themselves whereas the encrypted data say the cipher text are plainly visible for the hacker which will stimulate suspicion. Since steganography is meant for the concealment of information it can be used to protect both messages and communicating parties whereas cryptography protects only the contents of a message. Here, for embedding the secret key in an image, the least-significant bit insertion method (Chandramouli and Memon, 2001) is used. This is the simplest approach for hiding data within an image file where the binary representation of the hidden data is overwritten on to the LSB of each byte within the cover image.

Related work: A few research works that have been done for information security in MANETs, the various approaches of biometric security and multimodal biometrics are briefly presented here.

Xiao (2004) introduced a new strategy for authentication of mobile users. Each group has a cryptographic key which is used for communication within the group. Each user of the group has a profile which contains all the information on the ID holders and the group leader maintains the biometric templates of the group members. Instead of a central authentication server, the group leaders acted as distributed authenticators. But this system used fingerprints only for authentication and also if the fingerprint is compromised, the entire communication would be compromised. Also the uni-modal biometric systems are having many disadvantages over multimodal biometric systems and are explained by Sasidhar *et al*. (2010). They examined the accuracy and performance of multimodal biometric authentication systems using state of the art Commercial Off-The-Shelf products.

To avoid the disadvantages of uni-modal biometrics, Jagadeesan *et al*. (2010) projected an efficient approach based on multimodal biometrics (Iris and Fingerprint) for securing the entire communication between the users. At the same time authentication is not implemented in this system.

Since authentication plays an important role in mobile ad hoc networks Kwon and Moon (2008) proposed an authentication methodology that combines multimodal biometrics and cryptographic mechanisms for border control applications. Authentication is provided based on zero-knowledge and challenge-response techniques by Komninos *et al*. (2007) or biometric-based techniques explained by different authors as in Kim and Hong (2008); Humm *et al*. (2009); Anand *et al*. (2010); Kumar *et al*. (2011) and Chen *et al*. (2012). Even though, they used different combinations of multimodal biometrics in their systems, both security and authentication were not taken into account in their systems.

Also, once these biometric are compromised they would be rendered useless since these authors used the features of the biometrics as such. In order to get revocability the cancellable forms of the biometrics can be used for providing security and authentication. This was attained by combining biometrics, genetic algorithms and cryptography as suggested by Shanthini and Swamynathan (2010; 2011a; 2011b; 2011c). In these papers the different combinations of biometric are used along with genetic operators for providing data security, user authentication and revocability.

Proposed work: In our proposed Multimodal Biometric-based Secured Authentication System using Steganography (MBSASS), two biometric say, fingerprint and face are used to provide message security and user authentication. This system not only protects the message communicated between the users of high security applications of MANETs but also authenticates the sender in an implicit way.

Pre-processing of biometric and pre-key distribution:

Fingerprint biometrics: In this proposed model MBSASS, receiver's fingerprint-based cryptographic key is used for encrypting the actual data and the key needs to be distributed among the users before the transaction takes place. Initially the fingerprint images of the users are acquired using fingerprint sensors and are preprocessed as explained in Shanthini and Swamynathan (2011a).

Figure 1 shows the different pre-processing steps say Normalization, Enhancement, Binarization, finding an orientation field map, finding a region of interest, thinning, removal of H breaks and removal of spikes and finally the features are extracted from the fingerprint image. Finally spurious minutiae are removed from the extracted minutiae.

At the same time the core point of the fingerprint image and the orientation field are also calculated using the following steps and is shown in Fig. 2:

- Input image is enhanced (Chikkerur *et al*., 2004) in order to obtain a better image quality
- The enhanced image is segmented and background is separated from a fingerprint image
- Then the whole enhanced image filters with a complex filter
- A fast pixel-wise orientation field computation (Nilsson and Bigun, 2003) is done onto this filtered image
- The orientation field computed in step 4 is used to obtain a logical matrix where pixel is set to 1 if the angle of the orientation is <= 3.14 / 2
- Next, the complex filtering output of the enhanced fingerprint image which is calculated in step 3 is used to find the maximum value of complex filtering output where the pixels of logical image are set to 1
- Steps 5-6-7 are repeated for a wide set of angles say 3.14/2-3*α, 3.14/2-2*α, 3.14/2-1*α, 3.14/2, 3.14/2+1*α, 3.14/2+2*α, 3.14/2+3*α, where α is an arbitrary angle
- All the points found in step 8 are subdivided into subsets of points which are quite near each other. For each of this subset the subset with the greatest x-averaged coordinate is considered and the core point is the candidate with the greatest x-coordinate. This is a good approximation in standard fingerprint image

From the extracted fingerprint features, the cryptographic key is generated using genetic two-point crossover operation and is explained in Fig. 3. Since privacy of the biometrics has to be maintained, the fingerprint biometrics of the users are not distributed as such instead only the keys generated from the fingerprint biometrics are shared between the users before the transaction takes place.

Authentication is provided by using the face biometrics of the users and here in our proposed model Eigen face-based facial recognition algorithm is used for verification. In this process, a color based technique is implemented for detecting human faces in images. First, skin regions are separated from non-skin regions and then the human face within the skin regions is located, cropped and normalized. Once all the images are normalized the Eigen faces are generated and from that the mean image is created as explained in Shanthini and Swamynathan (2011b). The sample face image database is given in Fig. 4 and Eigen faces and mean image are shown in Fig. 5a and 5b respectively. This mean image is also shared among the users before the actual transaction takes place.

Securing the data and implementation of the system: The processes involved at sender are explained in Fig. 6.

The actual confidential data is secured by following the steps given below:

- All users' cryptographic keys generated from their own fingerprint biometric are shared among the users
- A mean image generated from all users' facial images using Eigen face-based recognition algorithm is shared among the users

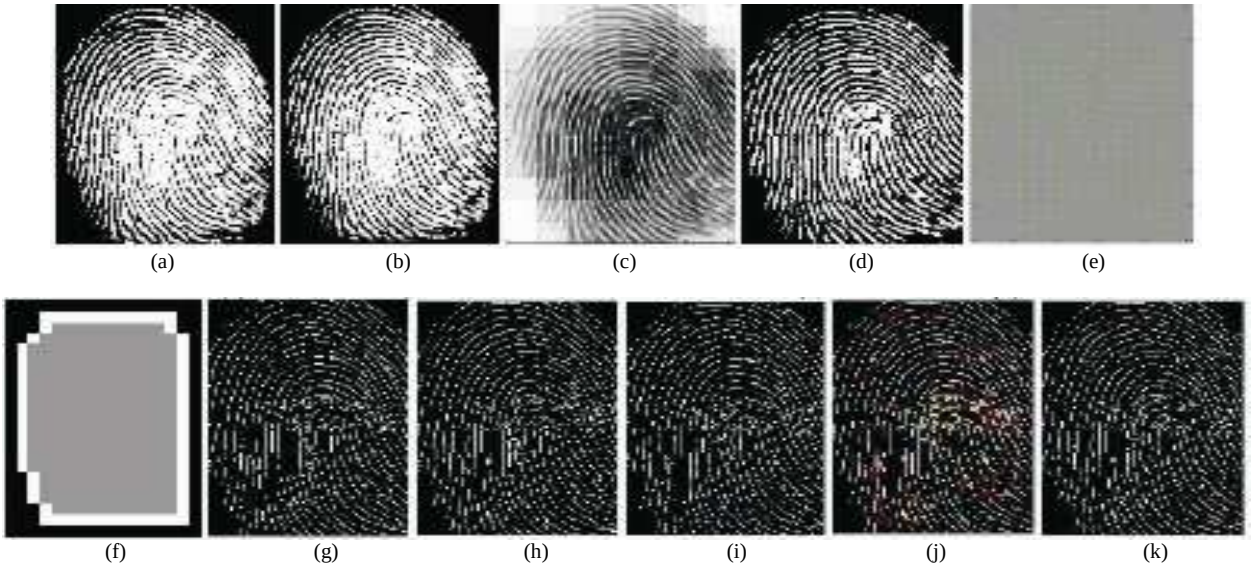


Fig. 1: Fingerprint pre-processing and minutiae extraction (a) Original image (b) Normalized image (c) Enhanced image (d) Binarized image (e) Orientation field map(f) Region of interest (g) Thinned image (h) Removal of H breaks (i) Removal of spikes (j) Extracted minutiae (k) Removal of spurious minutiae

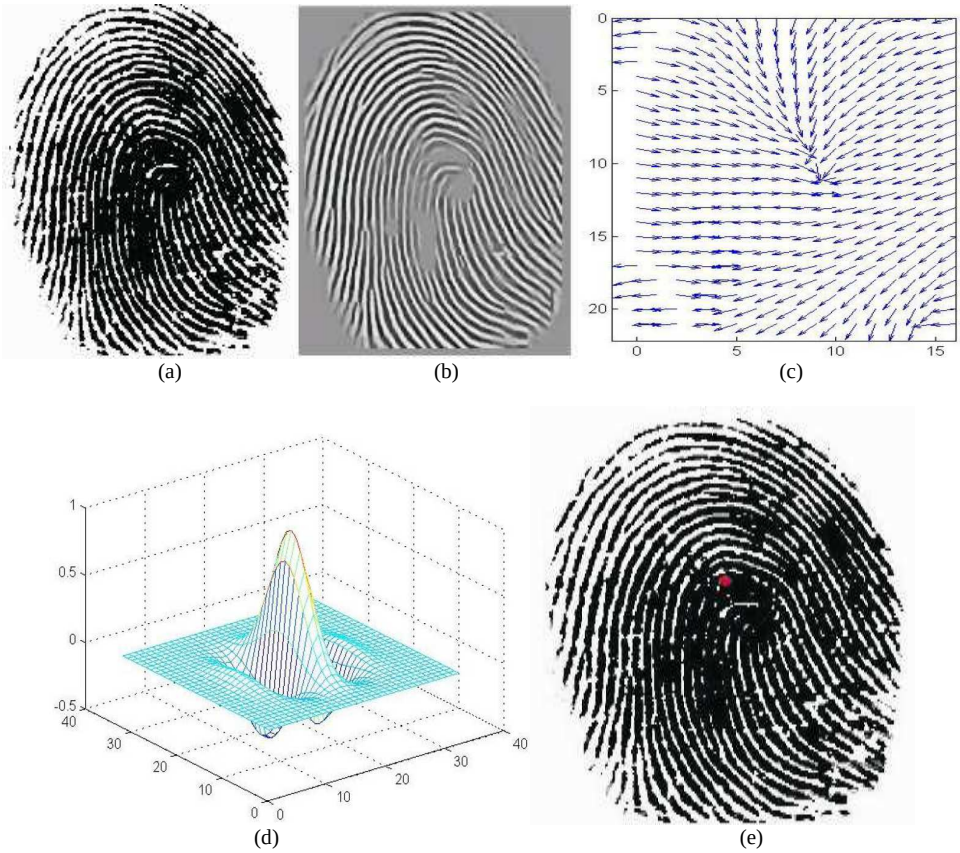


Fig. 2: Core Point Detection (a) Original Image (b) Enhanced Image (c) Orientation Field Map (d) Gabor Filtered Output (e) Image with Core Point

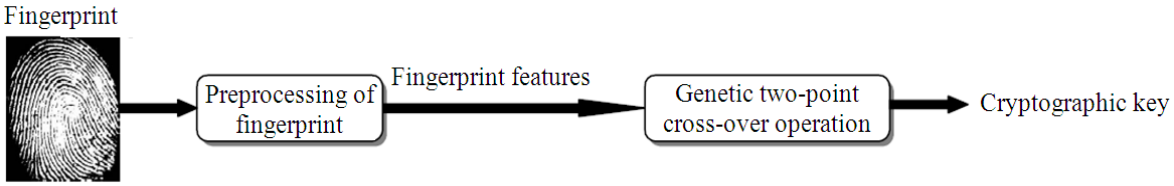


Fig. 3: Generation of cryptographic key

Fig. 4: Sample face image database

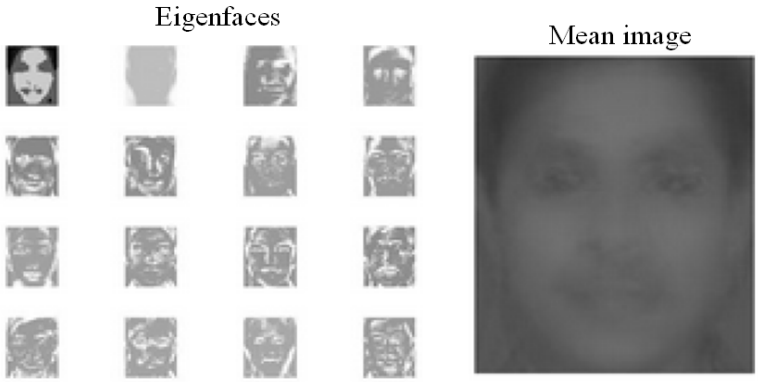


Fig. 5: (a) Eigen faces (b) Mean Image

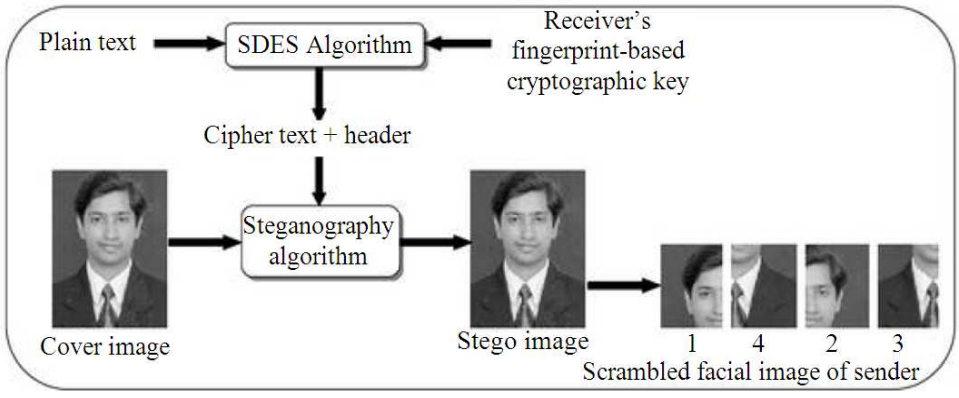


Fig. 6: Processes involved at sender

- Suppose if user A wants to send the confidential data to user B
- Actual message is encrypted by SDES algorithm using the receiver's fingerprint based cryptographic key to get the cipher text. Overview of SDES algorithm is given below.
- Sender's facial image is taken as the cover image for steganography. This cipher text and a header containing the core point, orientation field value and the no. of minutiae points are embedded in the cover image using the steganography algorithm say least-significant bit insertion method Chandramouli and Memon (2001). It is the easiest method where the least significant bit of each pixel of a gray-scale image used for embedding the message inside the image
- After applying the steganography algorithm the generated stage image is divided into 4 parts (No. of parts may be 8 or 16 or 64 as per the user) and is scrambled in the order 3, 2, 4 and 1. (It is assumed that this order is already shared among the users.) d. The scrambled images and a header containing the core point and no. of fingerprint features are transmitted to the receiver as shown in Fig. 5

User B receives the scrambled images in the same order and retrieves the data by applying the following steps:

- User B unscrambles the received images and separates the least significant bits from the stego image to get the cipher text and the header
- Then user B has to verify whether the received stego image belongs to the genuine training database by giving that image as the input to the facial recognition algorithm. It is transformed into its Eigen face component and for verification it is compared with the mean image. The verification process is explained in the following Eigen-face based recognition system. By this way, authentication is verified using facial biometric
- Once authentication is successful, the core point detection algorithm and feature extraction algorithm are applied onto user B's fingerprint image and the related details given in the header are found out and at the same time the no. of features extracted are also found out
- Displacement alignment and rotation alignment are done if the computed information is not matching with the header information
- If matched, the generated cryptographic key is used to decrypt the cipher text to get the original plain text. By this way, the data security is ensured because B's fingerprint can only decrypt the message

Overview of SDES algorithm: For encrypting the plain text a simple cryptographic algorithm, say, Simplified Data Encryption Standard (Stallings, 2010) is used. Even though the other algorithms like DES, AES and packet encryption system as specified in (Sengan and Pandian, 2012), are stronger than SDES the overhead also more compared to this and so we used SDES and the encryption and decryption algorithms are demonstrated in the Fig. 7a and 7b. The algorithm involves five functions: an Initial Permutation (IP); a Complex Function (CF) which involves both permutation and substitution operations depends on a key input; a simple permutation function (SW) that switches the two halves of the data; the Complex Function (CF) again; and finally a permutation function that is the inverse of the Initial Permutation (IP–1). The formula for encryption is:

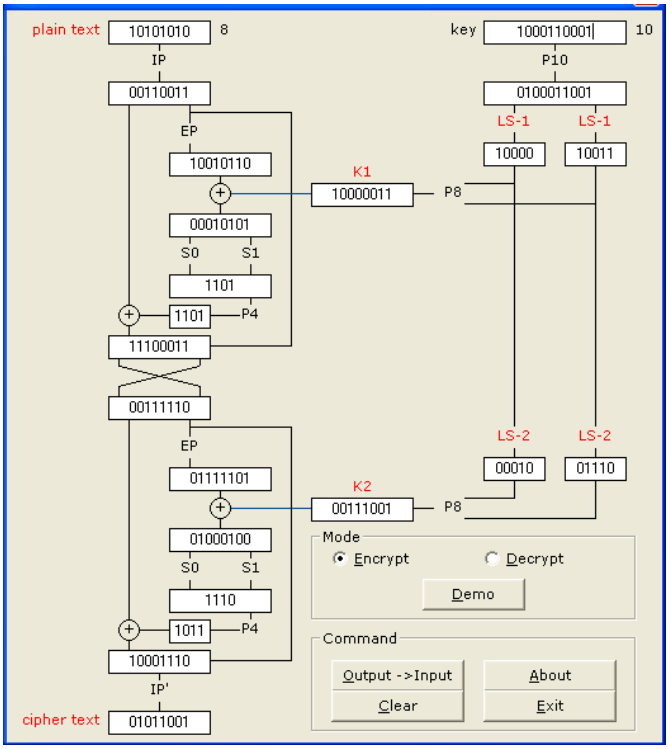
Ciphertext = IP-1 (CFK2 (SW (CFK1 (IP (Plain text))))) and decryption is essentially the reverse of encryption:

Plain text = IP-1 (CFK1 (SW (CFK2 (IP (Cipher text)))))

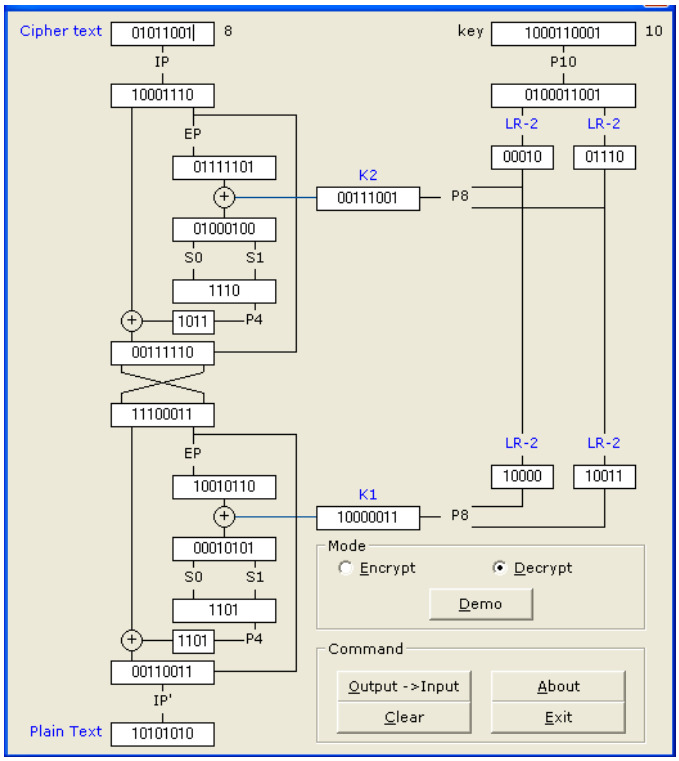
In the original version of S-DES, it depends on the use of a 10-bit key shared between sender and receiver. From this key, two 8-bit sub keys are produced for use in particular stages of the encryption and decryption algorithm. But in our proposed MBSASS model, the fingerprint based cancellable key, which is shared between the sender and receiver is used for encryption and decryption. Even though the algorithm is simple in nature to make it complex different 10-bit keys are used for different encryptions.

The proposed scheme can be implemented in any high security applications of MANET especially for a military scenario where short and confidential messages are sent that needs security as well as authentication.

Eigen-face based recognition system: A stego image is given as input to this system and is transformed into its Eigen face component. First our input image is compared with the mean image and their difference is multiplied with each eigenvector. Each value would represent weight and would be saved on a vector Ω.



(a)



(b)

Fig. 7: (a) SDES Encryption (b) SDES Decryptio

Table 1: Security related parameters

	Security parameters					
Encryption algorithm	Security - encryption	Authen tication	Priv acy	Revoc ability	Practi cality	Live ness
3DES192	Yes	No	-	No	No	No
AES-128	Yes	No	-	No	No	No
AES-256	Yes	No	-	No	No	No
GBBSSM	Yes	No	No	Yes	Yes	Yes
SASMBM	Yes	Yes	No	Yes	Yes	Yes
SASMVFB	Yes	Yes	No	Yes	Yes	Yes
MBSASS	Yes	Yes	Yes	Yes	Yes	Yes

$$\omega_k - u_x^t(T - \Psi)$$

where ω = weight, μ = eigenvector, Γ = input image, Ψ = mean face. The weight vector is given by:

$$\Omega^T = [\omega_1, \omega_2, ..., \omega_M]$$

Then which face class provides the best description for the input image is determined by minimizing the Euclidean distance:

$$\varepsilon_t = \left\| \Omega - \Omega_k \right\|^2$$

If ε_k is below an established threshold then the face image is considered to be a known face and it belongs to the training class. If the difference is above the given threshold, but below a second threshold, the image can be determined as an unknown face. If the input image is above these two thresholds, the image is determined not to be a face.

Security analysis:

Attacks countered by MBSASS:

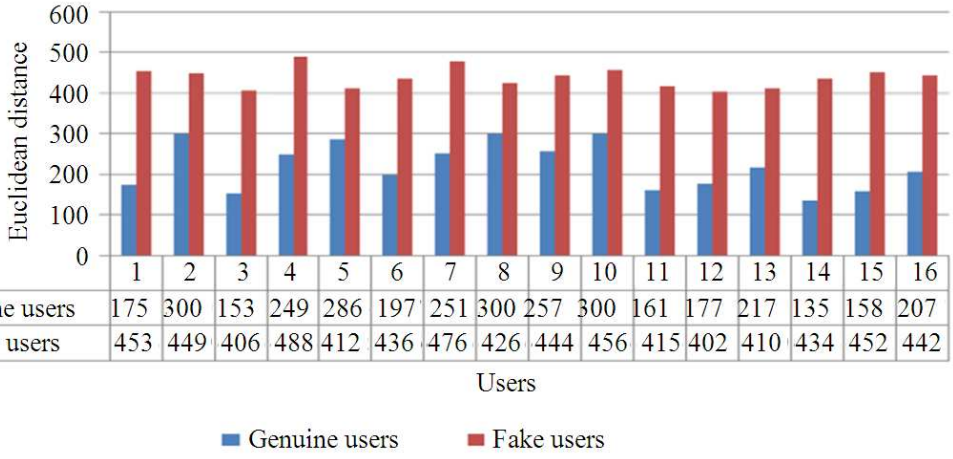
Exhaustive search attack: If the hacker does not have any information about the solution space or key statistics information, he has to perform an exhaustive search in the entire key space. If the key space is very large, the expected number of guesses by exhaustive search is also very large ie a longer key is more secure under exhaustive search attack. In the proposed MBSASS approach, since different key is used for different plaintext and every time the entire key space has to be searched it is computationally infeasible to get the key by this method.

Device key statistics attack: If the hacker knows the subject space of the system, he may probe the key generation system by inputting the subject information and collecting the statistics of the generated keys. Given such statistics, the hacker may have better ways to guess the cryptographic key. Since such attack focuses on the device the attack is named as a device key statistics attack. Our proposed MBSASS is intended to provide security for an application where a group of users will be allocated with independent devices and it is not at all possible to hack such system with this attack.

The security parameters of MBSASS: A brief comparison of some of the cryptographic algorithms based on security related parameters is given in Table 1. From the table we can understand that our MBSASS provides all security features compared to other algorithms say Triple DES, AES-128, AES-256, GBBSSM-64 (Shanthini and Swamynathan, 2010), SASMBM (Shanthini and Swamynathan, 2011c), SASMVFB (Shanthini and Swamynathan, 2011a).

The accuracy of the system is quantified for different combinations of face and fingerprint images in terms of False Acceptance Ratio (FAR), False Rejection Ratio (FRR), Genuine Acceptance Ratio (GAR) and Genuine Rejection Ratio. As a result of our proposed approach a GAR of 97.2% was obtained for an FRR of 1.21% whereas GRR and FAR was 0% for these databases.

Analysis of cryptography algorithm: Let us consider a known plaintext attack in which a single plain text (p1, p2, p3, p4, p5, p6, p7, p8) and its cipher text output (c1, c2, c3, c4, c5, c6, c7, c8) are known and the key (k1, k2, k3, k4, k5, k6, k7, k8, k9, k10) is unknown. (Stallings, 2010) Then each ci is a polynomial function gi of the pj's and kj's. We can therefore express the encryption algorithm as 8 nonlinear equations in 10 unknowns. There are a number of possible solutions, but each of these could be calculated and then analyzed. Each of the permutations and additions in the algorithm is a linear mapping. The nonlinearity comes from the S-boxes. It is useful to write down the equations for these S-boxes. For clarity, rename (p0,0, p0,1,p0,2, p0,3) = (a, b, c, d) and (p1,0, p1,1,p1,2, p1,3) = (w, x, y, z) and let the 4-bit output be (q, r, s, t) Then the operation of the S0 is defined by the following equations: q = abcd + ab + ac + b + d & r = abcd + abd + ab + ac + ad + a + c + 1 where all additions are modulo 2. Similar equations define S1. Alternating linear mappings with these nonlinear mapping results in very complex polynomial expressions for the cipher text bits make cryptanalysis difficult. To visualize the scale of the problem, note that a polynomial equation in 10 unknowns in binary arithmetic can have 210 possible terms. On average, we might therefore expect each of the 8 equations to have 29 terms. Once the key is found by brute-force attack, it is once for all rendered useless in any cryptographic algorithm.



	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Genuine users	175	300	153	249	286	197	251	300	257	300	161	177	217	135	158	207
Fake users	453	449	406	488	412	436	476	426	444	456	415	402	410	434	452	442

Fig. 8: Recognition of genuine users using Euclidean distance

But in our modified SDES, we change the 10 bit key for every encryption and so the key space expands in a considerable amount such that doing cryptanalysis is very difficult compared to SDES.

Also, if the users want to change the key they can apply another genetic operator to generate another key which can be shared among them for future use.

Analysis on face recognition system: In this experiment, the threshold value of the Euclidean distance of different number of faces was tested. In order to achieve this, a face library that contained nearly 32 face images, 16 genuine users and 16 fake users was used. All members of genuine users were in the training set then, the Euclidean distance of every member of the face library was found out. Figure 8 shows that the number of matches occurs when the threshold value is 300. It is seen from the figure that, 16 genuine members were classified 100% correctly and 16 fake members were not classified by this algorithm.

CONCLUSION

Conclusion and future work: Although biometric security is a very promising technology, challenges are slowing its development and deployment. Traditional security mechanisms are not sufficient for the applications where nodes are roaming in a hostile environment with relatively poor physical protection. Therefore to strengthen the encryption algorithm and key and for authentication the advantages of multi modal biometric, genetic algorithms and steganography are taken into our system. Secondly, security should be achieved by using simple algorithms like SDES that involve small inherent delays rather than complex algorithms which occupy considerable memory and delay. To add complexity, the keys used are changed for every encryption.

Fingerprint images and face images are chosen due to their unique physiological traits. In our systems either of these biometric has any mismatch the entire conversation is disapproved and banned. The method presented in this study remains as a preliminary approach to realize biometric security in applications which need high security and is designed for high security small group coalition operations and may not be suitable for enterprise usage. Multimodal biometrics can be used for multiple security services and this is proved in health care systems and ATM transactions. This property of providing different security services with different biometric modalities are compared.

REFERENCES

Anand, P.M.R., G. Bajpai and V. Bhaskar, 2010. 3D signature for efficient authentication in multimodal biometric security systems. Int. J. Eng. Technol., 2: 177-184.

Chandramouli, R. and N. Memon, 2001. Analysis of LSB based image steganography techniques. Proceedings of the International Conference on Image Processing, Oct. 7-10, IEEE Xplore Press, Thessaloniki, pp: 1019-1022. DOI: 10.1109/ICIP.2001.958299

Chen, C.L., C.C. Lee and C.Y. Hsu, 2012. Mobile device integration of a fingerprint biometric remote authentication scheme. Int. J. Commun. Syst., 25: 585-597. DOI: 10.1002/dac.1277

Chikkerur, S., C. Wu and V. Govindaraju, 2004. A systematic approach for feature extraction in fingerprint images. Biometric Authentication, 3072: 1-23. DOI: 10.1007/978-3-540-25948-0_48

Fessi, B.A., S.B. Abdallah, M. Hamdi and N. Boudriga, 2009. A new genetic algorithm approach for intrusion response system in computer networks. Proceedings of the IEEE Symposium on Computer Communication, Jul. 5-8, IEEE Xplore Press, Sousse, pp: 342-347. DOI: 10.1109/ISCC.2009.5202379

Humm, A., J. Hennebert and R. Ingold, 2009. Combined handwriting and speech modalities for user authentication. IEEE Trans. Syst. Man Cybernetics-Part A: Syst. Hum., 39: 25-35. DOI: 10.1109/TSMCA.2008.2007978

Jagadeesan, A., T. Thillaikkarasi and K. Duraiswamy, 2010. Cryptographic key generation from multiple biometric modalities: Fusing minutiae with iris feature. Int. J. Comput. Appli., 2: 975-8887.

Jain, A.K., P.J. Flynn and A.A. Ross, 2008. Handbook of Biometrics. 1st Edn., Springer, New York, ISBN-10: 038771040X, pp: 556.

Kim, D.S. and K.S. Hong, 2008. Multimodal biometric authentication using teeth image and voice in mobile environment. IEEE Trans. Consumer Elect., 54: 1790-1797. DOI: 10.1109/TCE.2008.4711236

Komninos, N., D.D. Vergados and C. Douligeris, 2007. Multifold node authentication in mobile ad hoc networks. Int. J. Commun. Syst., 20: 1391-1406. DOI: 10.1002/dac.882

Kumar, M.S.S., R. Swami and M. Karuppiah, 2011. An improved face recognition technique based on modular LPCA approach. J. Comput. Sci., 7: 1900-1907. DOI: 10.3844/jcssp.2011.1900.1907

Kwon, T. and H. Moon, 2008. Biometric authentication for border control applications. IEEE Trans. Knowl. Data Eng., 20: 1091-1096. DOI: 10.1109/TKDE.2007.190716

Li, S.Z. and A.K. Jain, 2005. Handbook of Face Recognition. 1st Edn., Springer Science and Business, New York, ISBN-10: 038740595X, pp: 395.

Maltoni, D., 2003. Handbook of Fingerprint Recognition. 2nd Edn., Springer, New York, ISBN-10: 0387954317, pp: 348.

Nilsson, K. and J. Bigun, 2003. Localization of corresponding points in fingerprints by complex filtering. Patt. Recogn. Lett., 24: 2135-2144. DOI: 10.1016/S0167-8655(03)00083-7

Ross, A.A., K. Nandakumar and A.K. Jain, 2006. Handbook of Multibiometrics. 1st Edn., Springer, New York, ISBN-10: 0387222960, pp: 198.

Sasidhar, K., V.L. Kakulapati, K. Ramakrishna and K.K. Rao, 2010. Multimodal biometric systems-study to improve accuracy and performance. Int. J. Comput. Sci. Eng. Survey, 1: 54-61. DOI: 10.5121/ijcses.2010.1205

Sengan, S. and S.C. Pandian, 2012. Secure packet encryption and key exchange system in mobile ad hoc nerwork. J. Comput. Sci., 8: 908-912. DOI: 10.3844/jcssp.2012.908.912

Shanthini, B. and S. Swamynathan, 2010. Data security in mobile ad hoc networks using genetic based biometrics. Int. J. Comput. Sci. Inform. Secur., 8: 149-153.

Shanthini, B. and S. Swamynathan, 2011a. A security system using genetic based face biometrics for MANETs. Proceedings of the International Conference on Intelligent Systems and Technology, (IST' 11).

Shanthini, B. and S. Swamynathan, 2011b. A Secure authentication system using multimodal biometrics for high security MANETs. Adv. Comput. Inform. Technol., 198: 290-307. DOI: 10.1007/978-3-642-22555-0_31

Shanthini, B. and S. Swamynathan, 2011c. A secured authentication system for MANETs using voice and fingerprint biometrics. Eur. J. Sci. Res., 59: 533-546.

Stallings, W., 2010. Cryptography and Network Security: Principles and Practice. 5th Edn., Prentice Hall, Upper Saddle River, N.J., ISBN-10: 0136097049, pp: 719.

Trivedi, A.K., R. Arora, R. Kapoor, S. Sanyal and A. Abraham *et al*., 2009. Mobile ad hoc network security vulnerabilities. IT Secur. Ethics.

Xiao, Q., 2004. A biometric authentication approach for high security ad-hoc networks. Proceedings of the 5th Annual IEEE SMC Information Assurance Workshop, Jun. 10-11, IEEE Xplore Press, pp: 250-256. DOI: 10.1109/IAW.2004.1437824

Zarza, L., J. Pegueroles and M. Soriano, 2007. Interpretation of binary strings as security protocols for their evolution by means of genetic algorithms. Proceedings of the 8th International Conference on Database and Expert Systems Applications, Sept. 3-7, IEEE Xplore Press, Regensburg, pp: 708-712. DOI: 10.1109/DEXA.2007.79