A LITERATURE SURVEY ON BIOMETRIC STEGANOGRAPHY USING VISUAL OBJECT FOR REMOTE AUTHENTICATION

Veda D[1], Bhargavi V[2], Harshitha S[3], Navyashree S[4]

[1]Asst Prof, Department of ISE, RajaRajeswari College of Engineering , Bangalore
[2,3,4]UG Students, ISE, RajaRajeswari College of Engineering, Bangalore

***Abstract*—Sensitive information is frequently exchanged via wireless network, which requires remote authentication for accessing the information. Remote authentication might be in the form of encrypted information. Intruder attacks such as Trojan Horse may cause serious issues especially in the case of remote operations. Here a robust authentication technique is proposed, which is based on Chaotic encryption and data hiding. If a user wants to be remotely authenticated, initially user has to select a video. Next, user's biometric signal is encrypted using a chaotic encryption method. Then the encrypted image is vectorized and the data hiding process is carried out using Qualified Significant Wavelet Trees (QSWTs). QSWT is used to achieve the invisibility, resistance to attacks and robustness in data hiding. Subsequently, the Inverse Discrete Wavelet Transform (IDWT) is applied to retrieve the hiddeninformation from the stego-object followed by an appropriate decryption process to get back the biometric image. Experimental results prove that the proposed technique would yield security merits and robustness to steganalytic attacks.**

***Index Terms*—Remote authentication, QSWT, Stego-object, Biometrics.**

INTRODUCTION

Authentication is the act of confirming the truth of an attribute of a datum or entity. This might involve confirming the identity of a person. The two main directions in the authentication field are positive and negative authentication. Positive authentication is well-established and it is applied by the majority of existing authentication systems. Negative authentication has been invented to reduce cyber-attacks. The difference between the two is explained by the following example: Password-based authentication. In positive authentication, the passwords of all users that are authorized to access a system are stored, usually in a file. Thus the passwords space includes only users passwords and it is usually limited (according to the number of users).If hackers receive the passwords file, then their work is to recover the plaintext of a very limited number of passwords. On the contrary, in negative authentication the anti-password space is created, (theoretically) containing all strings that are not in the passwords file. If hackers receive the very large anti-password file, their work will be much harder. This way, negative authentication can be introduced as a new layer of protection to enhance existing security measures within the networks.

The proposed scheme is a positive authentication system and for security reasons elements from at least two and preferably all three, of the following factors should be verified:

- the ownership factor: Something the user has

(e.g. ID card, security token, cell phone etc.)

- the knowledge factor: Something the user knows

(e.g., a password, a PIN, a pattern etc.)

- the inherence factor: Something the user is or does

(e.g., fingerprint, retinal pattern, DNA sequence, face, other biometric identifier etc.)

According to the case study mentioned in [4], the first two factors can easily be hacked by the intruders. So, the human authentication following the inherence factor would tend to give more security than the other factors, because the user inputs their own biometric image and it would make the attackers less to interpret or crack the authentication mechanism. Biometrics have already been incorporated in the remote authentication scheme [1,2,3], but only as password substitution in smart cards. Most of the password based authentication schemes are simple and the passwords can easily be guessed or broken [5], [6]. Moreover, it is most of the people's mentality to use the same password across different applications. Thus, if a malicious user determines a single password, it can be used to make attacks across multiple applications. Combination of encryption and steganography can achieve the biometric technique successfully. In particular, cryptographic algorithms can scramble biometric signals so that they cannot be understood.To confront the problem of user authentication, proposed an efficient wavelet-based steganographic method for biometric signals hiding in video objects, which focuses on optimizing the authentication rate of hidden biometric data over error prone transmissions. Interesting techniques for object-oriented data hiding have been presented forexample, however, most of them do not particularly consider the case of biometric data. Thus the main

contributions and novelties of the proposed system are as follows. (a) It is one of the first to use video objects to hide their respective biometrics[7]. By this way "dual" authentication is accomplished, the first by visual perception of the figured person, and the second by extraction and matching of the hidden pattern. (b) Biometric signals are encrypted before hiding. The statistical properties of this novel combination are analyzed and presented. (c) A DWT based algorithm is adapted for biometrics hiding. In contrast to most steganographic algorithms that are capacity efficient, the proposed algorithm is very robust to several types of signal distortions. By this way, the proposed scheme contributes to illustrate the perspective of encrypted biometrics authentication systems over error prone networks.

EXISTING SYSTEM

Password authentication with insecure communication

L. Lamport [8]had proposed a method on remote password authentication. Inorder to stop the intruders from hacking the system, a method called One way hash function was implemented.An algorithm that turns messages or text into a fixed string of digits, usually for security or data management purposes. The "one way"means that it's nearly impossible to derive the original text from the string. A one-way hash function is used to create digital signatures, which in turn identify and authenticate the sender and message of a digitally distributed message.In his scheme a verification table should be maintained On the remote server.

Advantages:

- It is secure even if an intruder can read the system's data, and can tamper with or eavesdrop on the communication between the user and the system.
- It is quick to compute the hash value for any given message.

Disadvantages:

- In this scheme a verification table should be kept on the isolated server and if burglars interruption into it, they can adapt the table.

A password authentication scheme over insecure networks

I.-E. Liao, C.-C.Lee, and M.-S.Hwang [10] had proposed a method which uses Diffie Hellman Key agreement protocol over insecure networks. It is a method for two computers which is used to generate a shared private key with which they can exchange information across an insecure channel. This shared private key is used to encrypt or decrypt the information by agreeing the session key.Which was of discrete logarithm problem computationally infeasible to calculate for large prime numbers.

Advantages:

- A shared private key is generated in order to exchange information through insecure channels.
- Their memory would retain data for up to 10 years without electrical power and they would support at least 10,000 read-write actions during the life of the card.

Disadvantages:

- Random cryptographic keys are difficult to memorize.
- Several passwords are simple and they can be easily guessed or broken.
- Most people use the same password across different applications; if a malicious user determines a single password, they can access multiple applications.

A more efficient and secure dynamic id-based remote user authentication scheme

Y.-y. Wang, J.-y.Liu, F.-x.Xiao, and J. Dan [9] Liao et al.'s scheme does not secure against some attacks. It means that the scheme cannot practically be used for smart card-based authentication applications.In these work dynamic users identities per transaction section could be used. These methods aimed to overcome a common drawback of older remote authentication schemes using smart cards,user's identity was static in all the transaction sessions.existing smart cards are vulnerable since the secret values stored in a smart card could be extracted by monitoring its power consumption. Therefore, we further assume that the attacker *A* can steal the user's smart card and extract the values stored in the smart card.

Advantages:

- The remote system does not need a dictionary of verification tables to authenticate users.
- Users can choose their passwords freely.

Disadvantages:

- It may leak some information about that user and can create risk of ID-theft during the message transmission over an insecure channel.
- Users should always have their smart cards with them in order to do transactions
- if a user loses his/her smart card, he/she will not be able to do any transactions and should wait for the reissuing of the card (sometimes several days).
- Smart cards cost money and effort each time they are (re)issued.
- Due to low power they cannot perform very complex computations

Dynamic id-based remote user password authentication schemes using smart cards

R. Madhusudhan and R. C. Mittal, [11] had reviewed a paper on password authentication for remote users which used smart cards this technique was based on dynamic id generated. Remote server verifies the identity of the user over the insecure communication channel. Many of the proposed

papers on remote authentication uses static id, which may leak some information about that user and can create risk of identity theft during the message transmission. Therefore in this paper the author uses dynamic id generation technique which has more security.In this section, we review six dynamic ID-based password authentication schemes, which are based on hash-functions. Each password authentication scheme is composed of four phases. They are registration phase, login phase, authentication phase and password change phase. In the registration phase, theuser U registers withtheremoteserverS and obtainsasmartcardthroughsecurechannelforfutureuse.In the loginphase,when User wants tologinto Server for usingresourcesof Server, heinsertshissmartcardintothecardreaderandkeysinhis identity ID and password PW to accessservices.Inthe authentication phase, Server verifies thevalidityofthelogin request.Password change phaseisinvoked,whenever the user wants tochange his password.Hecaneasilychangehispasswordwithouttaking any assistancefromtheremotesystem.

Advantages:

- Users can update their passwords after the registration phase.
- A session key agreed by the user and the remote system can be generated in every session.

Disadvantages:

- Smart cards cost money and effort each time they are issued or reissued.
- Due to low power they cannot perform very complex computations.
- users should always have their smart cardswith them in order to do transactions.
- If a user loses his/hersmart card, he/she will not be able to do any transactions andshould wait for the reissuing of the card.

An introduction to biometric recognition

K. Jain, Arun Ross, and SalilPrabhakar [12] proposed a paper on introduction to biometric recognition. All Systems require security that will be reliable personal recognition schemes that confirms the identity of an individual user requesting the service. The systems usually may includecomputer systems, laptops, cellular phones, ATMsas shown in (figure2). This paper uses the concept of biometrics to provide the security of systems.Biometric recognition or, simply, biometrics refers to the automatic recognition of individuals based on their physiological or behavioral characteristics. By using biometrics, it is possible to confirm or establish anIndividual'sidentity.A *biometric system* is essentially a pattern recognition system that operates by acquiring biometric data from an individual, extracting a feature set from the acquired data, and comparing this feature set against the template set in the database. Depending on the application context, a biometric system may operate either in *verification* mode or *identification* mode.

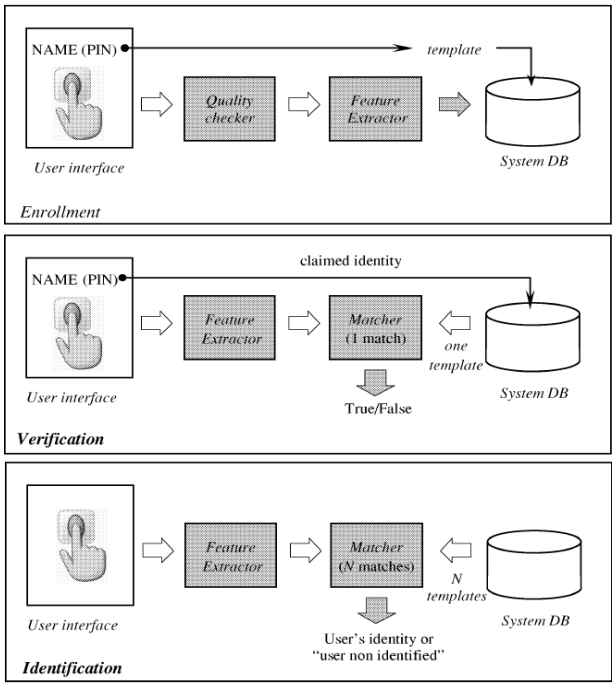

Fig 1: Block diagrams of enrollment, verification, and identification tasks of a biometric system.

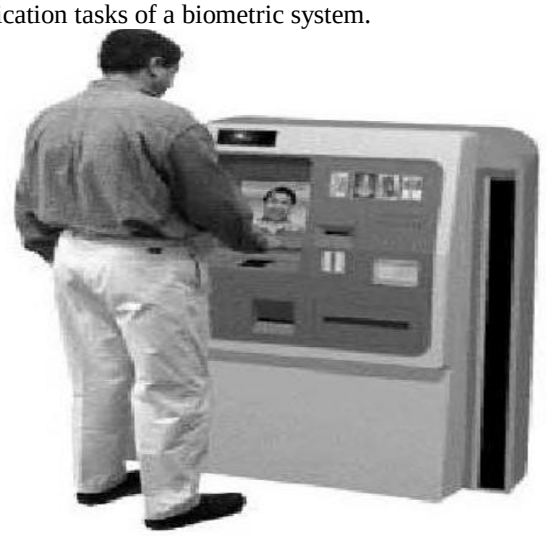

Fig 2: Biometric application used in ATM's

Advantages:

- Biometrics are inherently more reliable.
- Biometric traits cannot be lost or forgotten.
- They are more difficult to forge, copy, share, and distribute and they do not require the person being authenticated to be present at the time and point of authentication.

Disadvantages:

- Biometrics are used simply as an authentication tool in smart card technology.
- They cannot provide anonymity and three-factor security while they are vulnerable to the privileged insider and the user impersonation attacks.

Hide and seek: An introduction to steganography

N. Provos and P. Honeyman [13] proposed a concept on "steganography" which is defined as art and science of hiding communication. The process of hiding the data inside the image is called steganography, data can be of any kind like message, text, audio, video. This hidden data will be the secret information which has to be sent to the receiver. Information hiding generally relates to both watermarking and steganography. A watermarking system's primary goal is to achieve a high level of robustness that is, it should be impossible to remove a watermark without degrading the data object's quality. Steganography, on the other hand, strives for high security and capacity, which often entails that the hidden information is fragile.Even trivial modifications to the stego medium can destroy it. By doing the process of steganography the data will be hidden inside the image the resultant image obtained will be similar to that of input hence while transmission the hacker can't recognize the information hidden inside the image, hence the secret data will have more protection and it will be safe. Steganography will only be applied to secret information that has to be transmitted to remote user, so that while transmitting the hacker will not be able to hack the secret data. This paper reviews how steganography methods can be used to secure secret data.

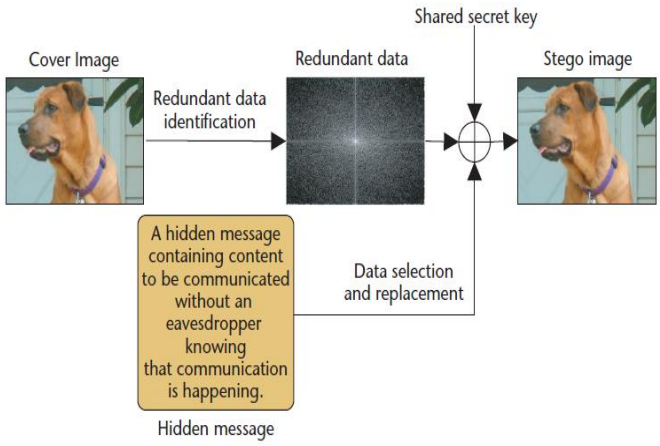

Fig 4:Modernsteganographic communication

The encoding step of a steganographic system identifies redundant bits and then replaces a subset of them with data from a secret message as shown in figure 4

Advantages:

- Data hidden will be secured.
- Any secret information can be sent across the insecure channel.
- Hackers cannot identify the data that is hidden inside the image. So it provides a high level of security.
- Useful in many applications where secret data has to be transferred to remote host.

Disadvantages:

- Difficult to detect the hidden data at the receiver side.

A DWT based Approach for Steganography Using Biometrics

Anjali.A. Shejul, U.L.Kulkarmi [14] proposed Discreet Wavelet Transform(DWT) algorithm for hiding the biometric image that is Steganography using Biometrics. The proposed paper provides high level of security for transmission on data in communication channel as it uses stegnography along with Biometrics. Here the secret data is embedded within the skin region of the image. The secret data which has been embedded inside the skin region of a person can't be recognized very easily. This skin tone detection is performed using HSV (Hue, Saturation and Value) color space. Additionally secret data embedding is performed using frequency domain approach - DWT (Discrete Wavelet Transform), DWT outperforms than DCT (Discrete Cosine Transform). Secret data is hidden in one of the high frequency sub-band of DWT by tracing skin pixels in that sub-band. Different steps of data hiding are applied by cropping an image interactively. Cropping results into an enhanced security than hiding data without cropping i.e. in whole image, so cropped region works as a key at decoding side.

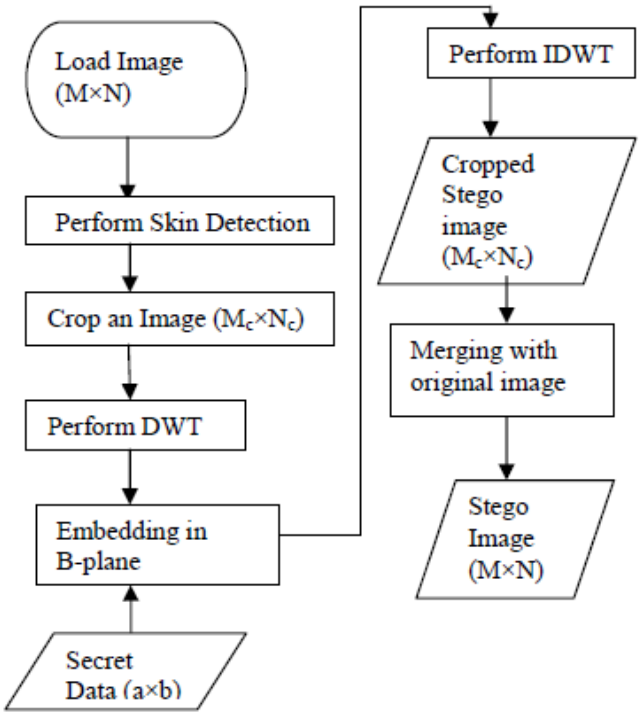

Fig 5:Flowchart of Embedding Process

The above figure 5 shows how the secret data is embedded within the skin region of a person's image. Initially loading of M*N size image is performed. Then recognition of skin region in the image further we chop the image afterwards the DWT process is performed. Next phase is embedding of secret data inside the cropped image which further has few process that is performing IDWT cropping the stego image merging with original image. Then obtained image is steganographed image.

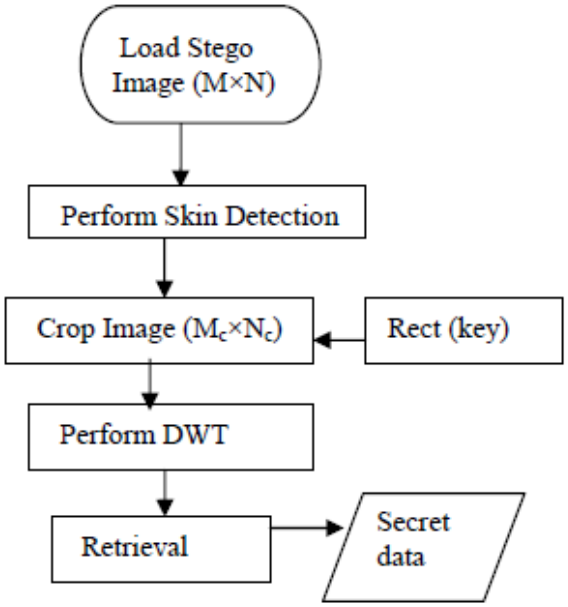

Fig 6: Flowchart of Extraction Process

The above figure 6 shows Extraction process that is regeneration of secret data and the cover image. Initially the stego image obtained loaded which is of size M*N. Further skin detection is performed, then we crop the image find the key ie the secret information then we perform DWT process. Finally the secret data will be retrieved.

Advantages:

- Messages do not attract attention to themselves.
- More secure as it uses both Biometrics and stegaonagraphy

Disadvantages:

- It can pose some serious problems as it is difficult to detect.

Region-BasedWatermarking of Biometric Images:Case Study in Fingerprint Images

K. Zebbiche and F. Kheli [15] reviewed a paper on region based watermarking of Biometric images. The proposed scheme embeds the watermark into the region of interest, thus it prevents the hidden data from segmentation process that removes the useless background and keeps the region of interest unaltered. It also provides more robustness and better imperceptibility of the embedded watermark. The proposed scheme is introduced into the optimum watermark detection in order to improve its performance. It is applied to fingerprint images, one of the most widely used and studied biometric data. The watermarking is assessed in two well-known transform domains: the discrete wavelet transform (DWT) and the discrete Fourier transform (DFT). The results obtained are very attractive and clearly show significant improvements when compared to the standard technique, which operates on the whole image. The proposed system working is as shown in the figures 7, 8.

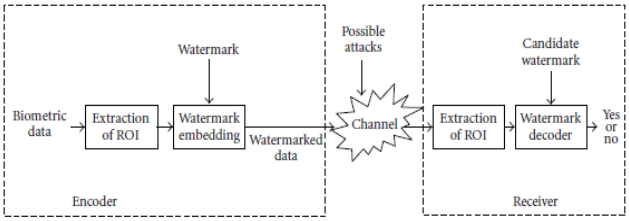

Fig 7: Proposed watermarking scheme for biometric data.

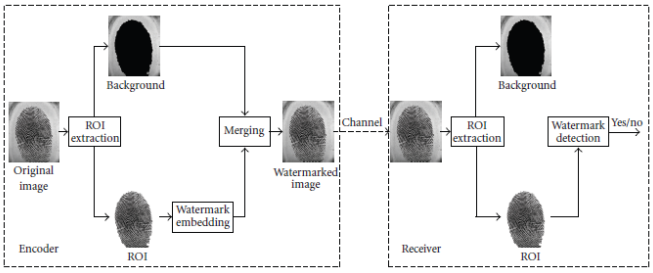

Fig 8: Personalized watermarking system applied to fingerprint images.

Advantages:

- Proposed method introduces a new method of embedding secret data within skin as it is not that much sensitive to HVS (Human Visual System).
- This takes advantage of Biometrics features such as skin tone, instead of embedding data anywhere in image, data will be embedded in selected regions.

Disadvantages:

- Reduces social sharing.
- Promotes negative image of the user.
- An obvious distraction.

CONCLUSION

The proposed technique yields best security in the authentication process. When an intruder tries to attack, he/she has to know if steganography is used in the authentication process. Even if the intruder knows the existence of steganography and tries to steal the stego image, he/she will end up with vectorised numbers. This would create a confusion to the cracker to decide what these numbers are.

Steganography by itself does not ensure secrecy, it is combined with a chaotic encryption system. Proposed procedure, outputs a stego-object that can resist different signal distortions, and steganalytic attacks. Results indicate that the use of QSWTs provides high levels of robustness, keeping at the same time the ease of implementation and the compatibility to well-known and widely used image and video. Lastly the system is able to recover the hidden encrypted biometric signal under different losses.

The application of the proposed system could be a smart interview system wherein a candidate can give an interview from a remote location using his face image and finger biometric.

ACKNOWLEDGEMENT

The authors would like to express sincere thanks forencouragement and constant support provided by theManagement RRGI, and Principal RajaRajeswari College ofEngineering, Bangalore-74, India during this research work.

REFERENCES

[1] E.-J. Yoon and K.-Y. Yoo, "*Robust biometrics-based multi-server authentication with key agreement scheme for smart cards on elliptic curve cryptosystem*", The Journal of Supercomputing, vol. 63, no. 1, Jan. 2013.

[2] M.-C. Chuang and M. C. Chen, "*An anonymous multi-server authenticated key* agreement *scheme based on trust computing using smart cards and biometrics*", Expert Systems with Applications, vol. 41, no. 4, Mar. 2014, pp. 1411–1418.

[3] H. Kim, W. Jeon, K. Lee, Y. Lee, and D. Won, "*Cryptanalysis and improvement of a biometrics-based multiserver authentication with key agreement scheme*", in Computational Science and Its Applications, ser. Lecture Notes in Computer Science, vol. 7335. Spinger-Verlag, 2012.

[4] "*Identity fraud report: Data breaches becoming a treasure trove for fraudsters*", Javelin Strategy and Research, Tech. Rep., 2013.

[5] M. Jakobsson and M. Dhiman, "The *benefits of understanding passwords*", in Mobile Authentication, ser. Springer Briefs in Computer Science. Springer New York, 2013, pp. 5–24.

[6] 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.

[7] S. Li and W. Li, "*Shape-adaptive discrete wavelet transforms for arbitrarily shaped visual object coding*", IEEE Transactions on Circuits and Systems for Video Technology, vol. 10(5), Aug. 2000, pp. 725–743.

[8] L. Lamport, "*Password authentication with insecure communication*,"Communications of the ACM, vol. 24, no. 11, pp. 770–772, 1981

[9] 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.

[10] 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.

[11] R. Madhusudhan and R. C. Mittal, ``*Dynamic ID-based remote user password authentication schemes using smart cards: A review*," *Intell.Algorithms Data-Centric Sensor Netw.*, vol. 35, no. 4, pp. 1235_1248, Jul. 2012.

[12] K. Jain, A. Ross, and S. Prabhakar, "*An introduction to biometricrecognition*," IEEE Transactions on Circuits Systems for Video Technology,vol. 14(1), pp. 4–20, 2004

[13] N. Provos and P. Honeyman, ``*Hide and seek: An introduction to steganography*," *IEEE Security Privacy*, vol. 1, no. 3, pp. 32_44, May/Jun. 2003.

[14] Anjali .A. Shejul, U. L. Kulkarni "*A dwt based approach for image steganography*,"International Conference on Data Storage and Data Engineering, 2010.

[15] K. Zebbiche and F. Kheli_, ``*Region-based watermarking of biometric images: Case study in fingerprint images*," *Int. J. Cryptography Inf. Secur.*, vol. 2008, Jun. 2008, Art. ID 492942.