www.ijecs.in
*International Journal Of Engineering And Computer Science ISSN:2319-7242*
*Volume 2 Issue 6 June, 2013 Page No. 1827-1833*

# FACE RECOGNITION USING EIGEN FACES AND TRANSMISSION OF HIDDEN DATA USING WATERMARKING AUTHENTICATION

***Bali Manohar***

Department of CSE, Central University of Karnataka, Gulbarga

bali.manohar2012@gmail.com

## *Abstract*

This paper presents an *efficient* Face Recognition Using Eigen Face approach and a novel scheme of protecting the hidden transmission of face biometrics using authentication Watermarking technique.

Face is a complex multidimensional visual model and developing a computational model for face recognition is difficult. The paper presents a methodology for face recognition based on information theory approach of coding and decoding the face image. Proposed methodology is a connection of two stages – feature extraction using principle component analysis and recognition using the feed forward back propagation Neural Network.

The proposed scheme uses watermark embedding algorithm. Compared with personal identification number codes, method in diverse application but their validity must be guaranteed. Watermarking technique provides solution to ensure the validity of biometrics; proposed scheme is composed of three parts: watermark embedding, data embedding and data extraction. One of the applications of our proposed scheme is verifying data integrity for images transferred over the internet.

**Keywords**: Authentication Watermarking, Hidden transmission, new fragile watermarking algorithm, Steganography, Eigen Face, Neural Network.

## Introduction

Biometrics based personal identification techniques that use physiological or behavioural characteristics are becoming increasingly popular compared to traditional token-based or knowledge based techniques such as identification cards, passwords, etc. One of the main reasons for this popularity is the ability of the biometrics technology to differentiate between an authorized person and an imposter who fraudulently acquires the access privilege of an authorized person [1][7]. Among various commercially available biometric techniques such as face, voice, fingerprint, iris, etc.,

the biometrics techniques offer automated biometrics authentication techniques such as passwords and provides a convenient way and reliable method for personal identification, the problem of security and integrity of the biometrics data poses new issues. For example, if a person's biometric data is stolen; it is not possible to replace it as compared to replacing a stolen credit card, identification card or password. Schneider [2] points out that, a biometric based verification system can guarantee that the biometric data came from the legitimate person at the time of enrolment.

In order to promote the wide spread utilization of biometric techniques, an increased level of security of biometric data is necessary [3].

Watermarking is a popular technique that is used for copyright protection and authentication. This embeds data into digital contents such as text, video images and audio data without degrading the overall quality of the digital media[5]. A watermark is the information is to be hidden and also indicates that hidden information is transparent, the

watermarked data is the media which contains the watermark. The difference between watermarking and other technology is of three important aspects: Firstly, unlike encryption, watermark is imperceptible so that the image will not be detract from the aesthetic sense. Secondly, the watermarks and the works they embedded in are inseparable. Even if the works were displayed or converted into other file formats, the watermark will not be eliminated. Finally, the watermark will have exactly the same transformation experience as one sent by sender after adding data. The performance of any watermarking technique can be evaluated by considering the factors such as: capacity, robustness and visibility. Watermarking techniques can be divided in various ways, depending on the property that is taken into account. If we refer to the type of document, the host data can be images, audio, text or video files. According to application we can refer to source based methods and destination based methods. Based on human perception we can divide the watermarking algorithms as visible or invisible.

There are many techniques for hiding data or message in image such a manner that the alterations made to the image are perceptually indiscernible. Common approaches of steganography include [4]: Least significant bit insertion (LSB), Masking and filtering, and Transform techniques. Stenographic techniques have various features which characterize their strengths and weaknesses, the features include: Embedding capacity, perceptual transparency, robustness, tamper resistance and computational complexity.

## PROPOSED SYSTEM ARCHITECTURE

A proposed scheme of face recognition using Eigen faces and authentication watermarking for protecting hidden transmission of biometric is composed of three parts namely, watermark embedding model, data embedding model and data extraction model.

### *A. The Eigen Face Approach*

In the language of information theory, we want to extract the relevant information in a face image, encode it as efficient as possible, and compare one face encoding with a database of models encoded similarly.

In mathematical terms, we wish to find the principal components of the distribution of faces, or the eigenvectors of the covariance matrix of the set of face images, treating an image as appoint in a very high dimensional space.

These eigenvectors can be thought of as a set of features that together characterize the variation between the face images. Each image location contributes more or less to each eigenvector as a sort of ghostly face which we call an Eigen face. Each individual face can be represented exactly in terms of a linear combination of Eigen faces. Each Eigen face can also be approximated using only the best Eigen faces those that have the largest Eigen values, and which therefore account for the most variance within the set of face images.

This approach to face recognition involves the following initialization operations:

1. Acquire an initial set of face images(the training set)
2. Calculate the Eigen faces from the training set keeping only the M images corresponding to the highest Eigen values. These M images define the face space.
3. Calculate the corresponding distribution in M dimensional weight space for each known individual, by projecting their face images onto the face space.

Having initialized the system, the following steps are then used to recognize new face images:

1. Calculate a set of weights based on the input image and the M Eigen faces by projecting the input image onto each of the Eigen faces.
2. Determine if the image is a face at all by checking to see if the image is sufficiently close to face to face.
3. (Optional) update the Eigen faces and/or weight patterns.
4. (Optional) if the same unknown face is seen several time, its characteristic weight pattern and incorporate into the known faces.

*Calculating the Eigen Faces*

The system is initialized by first acquiring the training set (ideally a number of examples of each subject with varied lighting and expression). Eigenvectors and eigenvalues are computed on the covariance matrix of the training images. The M highest eigenvectors are kept. Finally, the known individuals are projected into the face space, and their weights are stored. This process is repeated as necessary. These images are converted from 256 by 256 images into a single dimension vector of size 65,536. This conversion is necessary because we need a 2-D square matrix to compute eigenvectors.

The mean of the training images (Γ1, Γ2, ΓM) is the "average face" Ψ = 1 M PM n=1 Γn. Each training image differs from the average face by Φi = Γi − Ψ. The vectors uk and scalars λk are the eigenvectors and eigenvalues of the covariance matrix of the face images Φi

The Eigen values $\lambda_k$ are selected such that

$$\lambda_k = \frac{1}{M} \sum_{n=1}^{M} (u_K^T \varphi_n)^2 \qquad (1)$$

The vectors $u_k$ and $\lambda_k$ are the Eigen vectors and Eigen values, respectively the covariance matrix

$$C = \frac{1}{M} \varphi_n \varphi_n^T = AA^T \qquad (2)$$

*B Watermark embedding:* In this model, we are embedding watermark data to the original host image using the new fragile watermarking algorithm. The host image may be signature face or any biometric identification. The result of this is the watermarked image as shown in Fig.1.

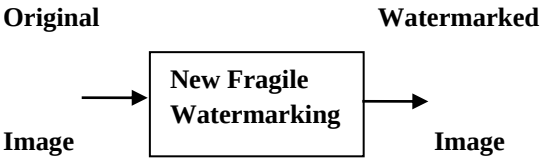



**Fig 1 Fragile Watermarking Algorithm**

In this algorithm, we propose a novel new fragile watermarking for JPEG image[16]. This is an extension of an existing CWSA algorithm. A fragile watermark is a watermark that is readily altered or destroyed when the host image is modified through a linear or nonlinear transformation. The sensitivity of fragile marks to modification leads to their being used in image authentication. A Fragile watermarking systems are categorized into two categories according to the working domain. First, fragile watermarking that works directly in the spatial domain [10][11].Second fragile watermarking that works in a transform domain.

It performs watermarking directly the JPEG quantized DCT coefficients and using robust chaotic functions to improve its cryptographic characteristics as shown in Fig.1.1.This has some features such as:

$$x\,(n+1) = F\big(x(n)\big) = \begin{cases} X(n), \frac{1}{p}\ 0 \le x(n) < p \\ [x(n) - p\,]. \frac{1}{0.5 - p}\,, p \le x(n) < 0.5 \\ F\big(1 - x(n)\big), 0.5 \le x(n) < 1 \end{cases}$$

This algorithm uses two chaotic generators. We propose the use of a Piecewise Linear Chaotic Map (PWLCM) for chaotic system1 [12] and a cascaded recursive filter with the skew tent non-linear function for the chaotic system2 [13]. The PWLCM is a chaotic function composed of multiple linear segments:

The chaotic system2 is composed of two cascaded recursive filters with non-linear function [14].

$$x(n+1) = F\big(x(n)\big) = \begin{cases} \frac{1}{a}, 0 \le x(n) \le a \\ \frac{1}{a-1}, x(n) + \frac{1}{1-a}, a < x(n) \le 1 \end{cases}$$

It embeds the watermark information both on the DC coefficient and on those AC coefficients with a value greater than a threshold T.

In this scheme, the initial value of the chaotic system2 is obtained using part of the secret key:

$$x_0 = F\,(\,f_{qc} + k_{x0})$$

Where $x_0\ is$ the initial is value of the chaotic system2, $f_{qc}$ is the analyzed coefficient with the LSB plane set to 0 and $k_{x0}$ is part of the secret key.

In this way the attacker will not have access to the initial value of the chaotic map.

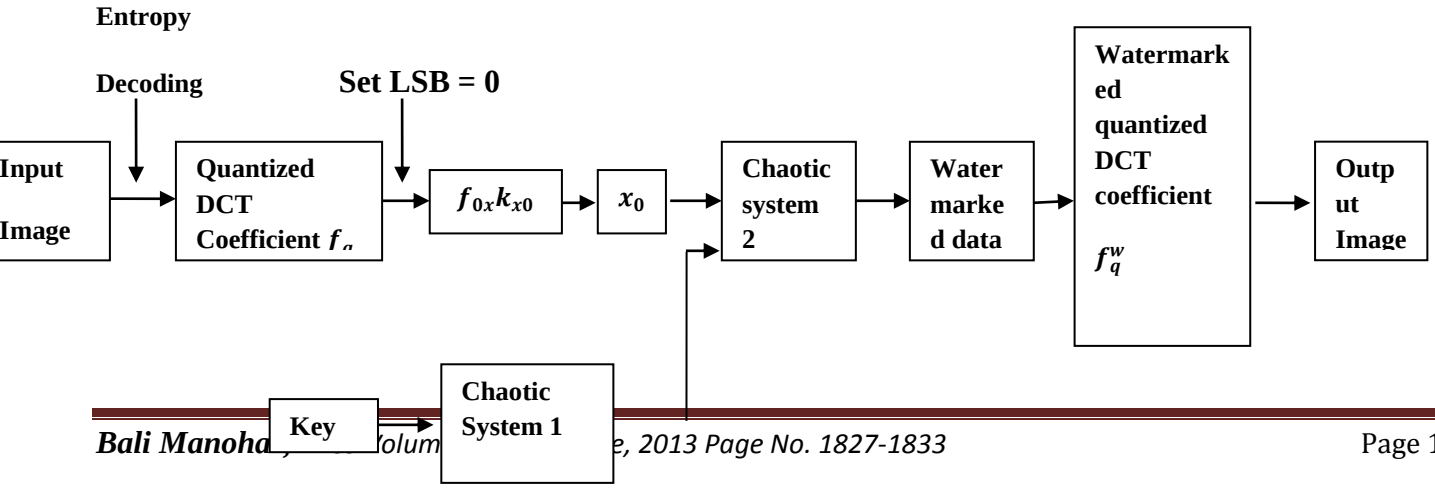


**Fig 1.1 Watermark Embedding process Using Fragile Algorithm**

*C. Data Embedding*

For hiding the data, a user name and password are required prior to use the system. Once the user login to the system, the user can use the information together with the secret key to hide the data inside the chosen image. Using a steganography algorithm, these data will be embedded and hided inside image with almost zero distortion of the original image as shown in Fig.2.

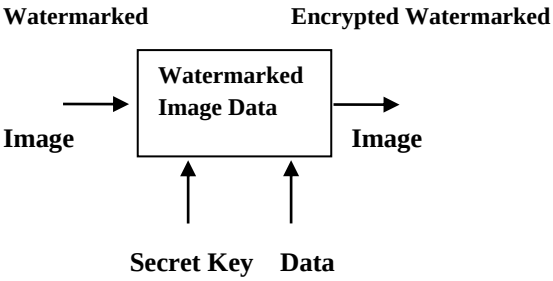



**Fig 2 Data Embedding Process**

*D. Data Extraction*

To retrieve data a secret key is required which is embedded in image. An unauthorized user without secret key receives tampered data. So, this ensures integrity and confidentiality of the data as shown in Fig.3.

*Least-Significant-Bit:* A digital image consists of a matrix of colour and intensity values. In a typical grey scale image, 8 bits/pixel are used. In a typical full-colour image, there are 24 bits/pixel, 8 bits assigned to each colour components. The simplest stenographic techniques embed the bits of the message directly into the least-significant-bit plane of the cover image in a deterministic sequence.

Modulating the least-significant-bit does not result in a human-perceptible difference because the amplitude of the change is small. Other techniques "process" the message with a pseudorandom noise sequence before or during insertion into the cover image. The advantage of LSB embedding is its simplicity and many techniques use these methods [15]. LSB embedding also allows high perceptual transparency. However, there are many weaknesses when robustness, tamper resistance, and other security issues are considered. LSB encoding is extremely sensitive to any kind of filtering or manipulation of the steno-image. Scaling, rotation, cropping, addition of noise, or lossy compression to the steno.-image is very likely to destroy the message. Furthermore an attacker can easily remove the message by removing (zeroing) the ntire LSB plane with very little change in the perceptual quality of the modified steno-image.

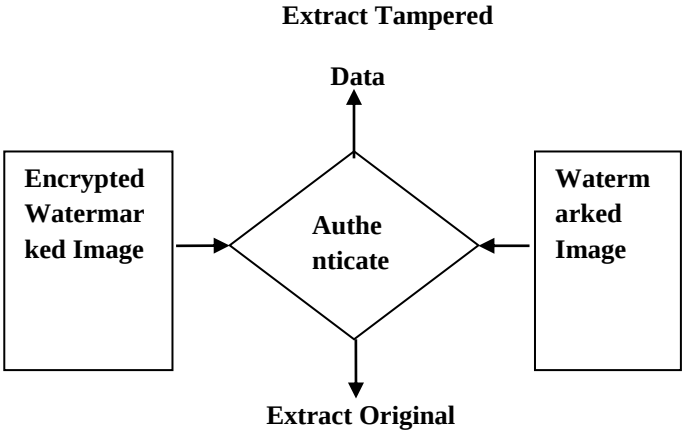



**Fig 3 Data Extraction Process**

## Experimental Results and Discussion

Firstly, the face image input is recognized by face recognition system as shown in figure 4. The recognized Face image is embedded with watermark data and the resultant output image is as shown in Fig.4 (a), Fig.4 (b) and Fig.4(c) respectively.

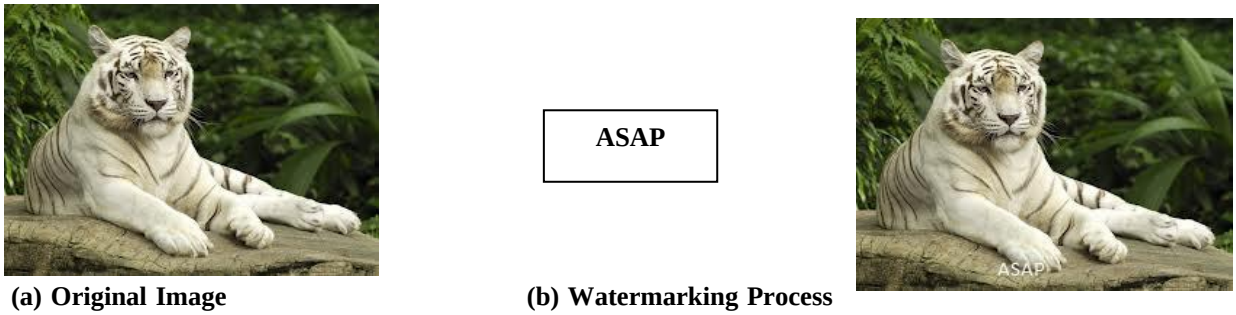
The resultant output image returned from Fig.4 is used for data embedding process using steganography technique. The Fig.5 shows the detailed approach followed and final output image is called stego image or cover image. Similarly Fig.6 shows the data extraction process carried out on the receiver end. Finally the watermarked image and message are separated. In this experiment, we found that the size of information to be hidden relatively depends on the size of the cover-image. The message size must be smaller than the image. A large capacity allows the use of fixed size, and thus decreases the bandwidth required to transmit the stego-image.

As shown in Fig.5, the watermarked image with our proposed new fragile watermarking algorithm is less distorted then the watermarked image using the CWSA algorithm. This is mainly due to the choice of the watermarked coefficients. The original CWSA algorithm embeds the watermark data on all AC coefficients. This makes it slow, because of the large number of coefficients that need to be processed and makes the modification to the image visible. We propose to embed the watermark both on the DC and AC coefficients with a value greater than a threshold.

The project which has been developed and proposed for the future work will give raise to the new trend in the information security by using the biometric methods. We propose a new concept in the information security using biometrics which is combination of data authentication, privacy and security.

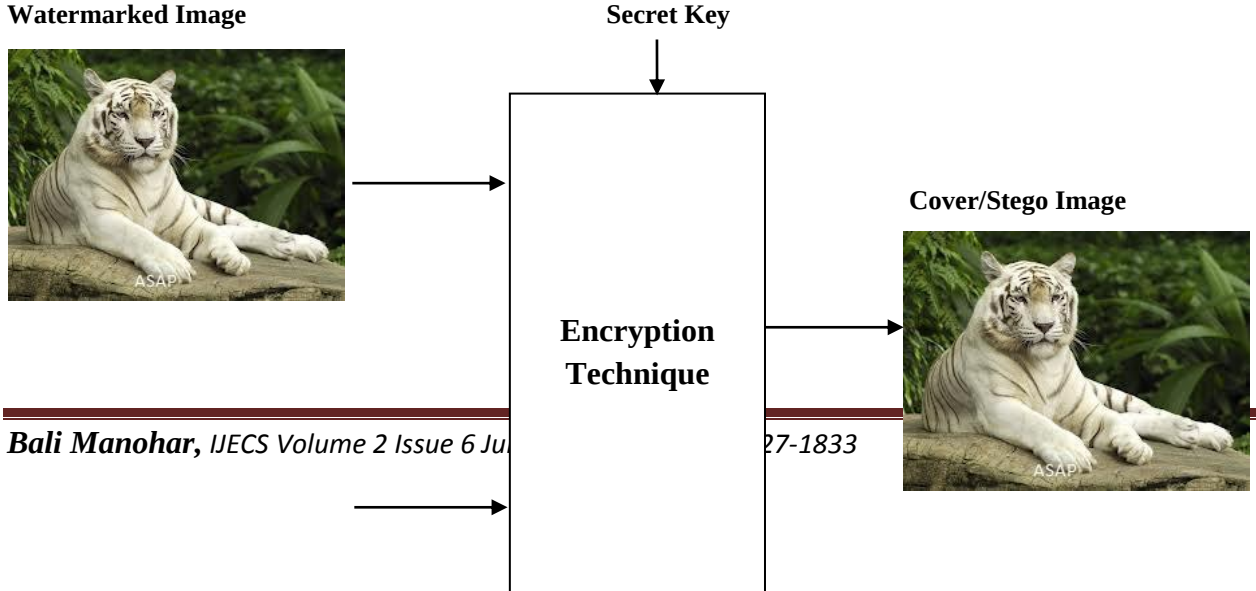

**Input Face Image** **Recognized Image**

**Figure 4 Face Recognition Systems**




**(a) Original Image** **(b) Watermarking Process** **(c) Watermarked Image**

**Figure 5 Watermark Embedding Process**



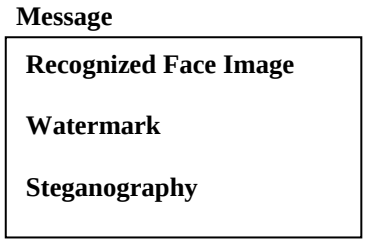



**Figure 5 Data Embedding Process**

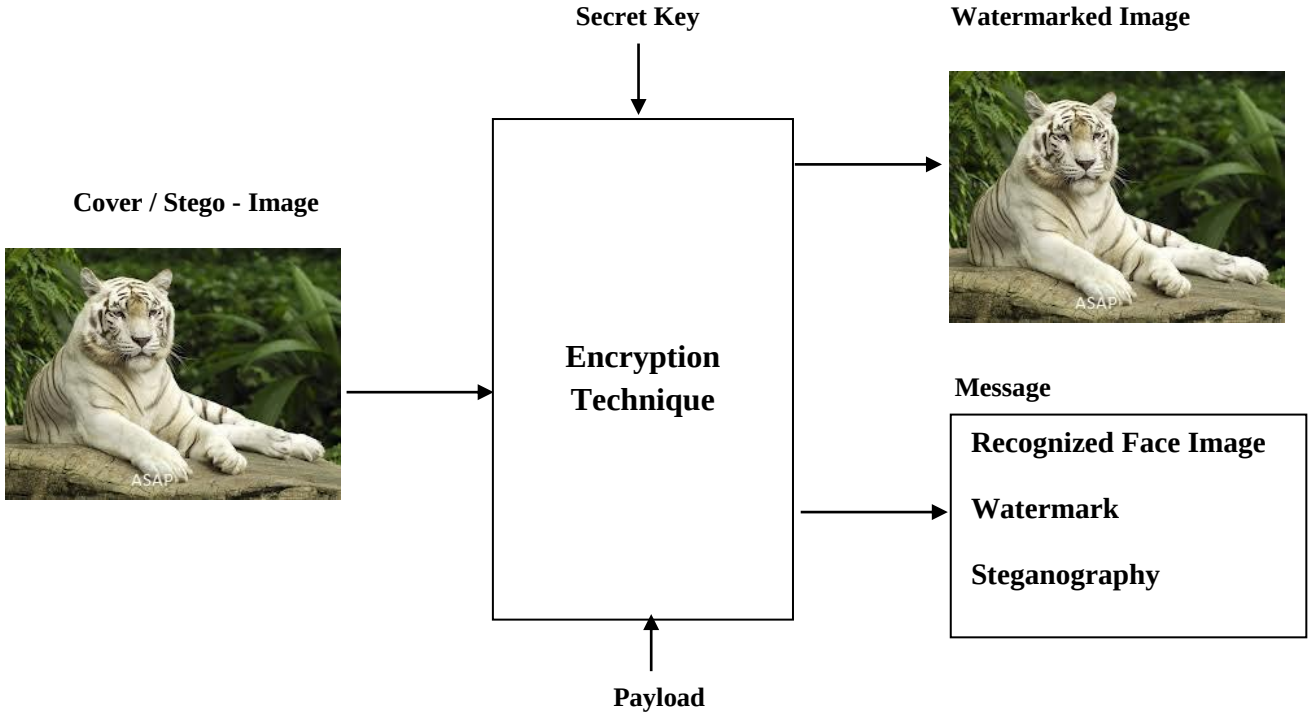



**Figure 6 Data Extraction Process**

## Conclusion

In our proposed scheme, initially we recognize the face image and then use the recognized face image to make it hide. A new fragile watermarking algorithm is used to convert the original host image into watermarked image. Then we applied steganography technique to hide the data in digital media for confidentiality of information and provide a means of communicating privately. The experiment results demonstrate that our proposed scheme protects hidden transmission of biometrics this can be used for any biometrics data e.g. fingerprint, iris, signature etc. The proposed application is used to ensure the data integrity over the images transferred on the internet.

## REFERENCES

[1]A. Jain, S. Pankanti, and R. Bolle, eds., Kluwer,"BIOMETRICS: personal identification in networked society", 1999.

[2]B. Schneier,"The uses and abuses of biometrics", Comm. ACM, vol.42, no.8, pp.136, Aug, 1999.

[3]N. K. Ratha, J. H. Connell, and R. M. Bolle,"An analysis of minutia matching strength", Proc Third AVBPA, Halmstad, Sweden, pp.223-228, June 2001.

[4]N. F. Jonson, S. Jajodia,"Steganalysis: The investigation of Hiding Information", IEEE, pp.113-116, 1998.

[5]S.jain, "digital Watermarking techniques: a case study in fingerprint & face ",Pmc.ICVGIP 2000, Bangalore, India, pp.139-144, Dec.2000.

[6]N. K. Ratha, J. H. Connell, and R. M. Bolle,"Secure data hiding in wavelet compressed fingerprint images", Proc. ACM Multimedia 2000 workshops, Los Angeles, CA. pp:127-130, 2000.

[7]M. K. Khan, J. S. Zhang, L. Tian, "Chaotic Secure Content based Hidden Transmission of Biometric Templates", Chaos, Solitons, Fractals, Vol.32, No.5, pp:1749 1759, 2007.

[8]Anil K J, U. Uludag, and R. L. hsu,"Hiding a face in a fingerprint image", Proceedings of International Conference on Pattern Recognition 2002, pp: 756-759, 2007.

[9]Anil K J, U. Uludag,"Hiding Biometric Data", IEEE Transaction on Pattern Analysis and Machine Intelligence, Vol.25, No.11, and pp: 1494 1498, 2003.

[10]Zaho Y.,"Dual Domain Semi-Fragile watermarking for Image Authentication", Master Thesis, University of Toronto, 2003.

[11]Walton S.,"Information Authentication for A Slippery New Age", Dr.Dobbs Journal, vol.20, no.4, pp.18-26, 1995.

[12]S. Li. G. Chen, X. Mou,"On the Dynamical Degradation of Digital Piecewise Linear Chaotic Maps", International Journal of Bifurcation and Chaos, 2005.

[13]S.EI Assad, H. Noura, I. Taralova, Design and analysis of efficient chaotic generator for cryptosystems Lecture notes in IAENG Transaction on Electrical and Electronical Engineering, vol.1, 2008, 10 pag.

[14]H. Noura, S. Henaff, I. Taralova et S.EI Assad, Efficient cascaded 1-D and 2-D chaotic generators, Second IFAC Conference on Analysis and Control of Chaotic System Chas, 2009.

[15]M.Z. I. Shamsuddin,"Menggunakan Least Significant Bit: Stegnografi", 2002.

[16]Daniel Caragata, Anca Livia Radu, Safwan EI Assad ,"Fragile Watermarking using Chaotic Sequence", International Journal for Information Security Research (IJISR),volume 1, Issue 1, March 2011.

[17]M. M Amin, M. Salleh, S. Ibrahim, M.R.K atmin, and M.Z.I. Shamsuddin", National Conference on excommunication Technology Proceedings, Shah Alam, Malaysia 0-7803-7773-7/03/$17.00 0 2003.

[18]Shumin Ding,Chunlei Liy,Ahoufeng Liu,"Protecting Hidden Transmission of Biometrics using Authentication Watermarking", 978-0-7695-4080, 2010.

[19]M. Iwata, K. Miyake, A. Shiozaki,"Digital watermarking method to embed index data in JPEG images", IEICE Trans. on Fundamentals, vol.E85-A, no.10, pp.2267-2271, October 2002.