ISSN: 0975-766X
CODEN: IJPTFI
Available Online through *Research Article*
www.ijptonline.com

HUMAN ORIENTED AUTHENTICATION USING FINGERPRINT RECOGNITION FOR SECURE ENVIRONMENT

[1]J.Senthil, [2]Dr.G.Singaravel
[1]Research Scholar, Bharath Institute of Higher Education and Research,
Bharath University, Chennai.
[2]Professor and Head, K.S.R College of Engineering (Autonomous), Tiruchengode.
Email: senthilgobi05@gmail.com

Received on: 15.10.2016 *Accepted on: 22.11.2016*

Abstract

This paper proposes a feature-based robust information exchange using Lempel Ziv Terry Welch(LZW) and Complex Hadamard Transform (CHT) algorithm is proposed to achieve the goal of text and image authentication and protection simultaneously. The first step is to identify the feature key areas for embedding. It is a novel robust image feature which can be seamlessly combined with the proposed key-dependent triangulation scheme. A random pre-warping framework is adopted to make the scheme robust to collusion attack. The experiments were conducted with and without attacks and was proved that the algorithms are able to resist the attacks. A comparison between the two feature selection algorithms was also performed based on the number of feature points detected with and without attacks. Both the algorithms prove that they are efficient in terms of fingerprint embedding and extraction and can resist various image processing and geometric attacks. Protection of biometric data is gaining interest and digital fingerprinting techniques are used to protect the biometric data from either accidental or intentional attacks. Among the various biometrics, iris is very famous in the authentication area, as they are unique to each person and are mainly used for the establishment of instant personal identity.

I. Introduction

However, it has also introduced serious concern on the protection issues, that is, individuals, other than the owner, may manipulate, duplicate or access media information illegally without the owner's consent and knowledge (Lin, 2000) [1]. This has forced academicians, industrials and researchers to focus on copyright protection of the intellectual contents. Accurate identification of a person could deter crime and fraud, streamline business processes, and save critical

resources. Here are a few mind boggling numbers: about one billion dollars in welfare benefits in the United States are annually claimed by "double dipping" welfare recipients with fraudulent multiple identities [33]. As the need for security increases, research for more permanent form of biometric which is difficult to replicate is considered. One such biometric is human iris. Iris recognition is based on visible features, i.e. rings, furrows, freckles and corona and is considered very challenging as they possess a high degree of randomness. The Iris is essentially formed by 8 months, and remains stable through life. It is proved statistically that iris is more accurate than even DNA matching as the probability of 2 irises being identical is 1 in 10 to the power of 78 (Daugman and Downing, 2001), [4]. During transmission, however, they are susceptible to accidental and intentional attacks, which emphasize the need for a protective scheme to preserve fidelity and prevent alterations. This paper proposes fingerprint as a solution to this situation. MasterCard estimates the credit card fraud at $450 million per annum which includes charges made on lost and stolen credit cards: unobtrusive positive personal identification of the legitimate ownership of a credit card at the point of sale would greatly reduce the credit card fraud; about 1 billion dollars worth of cellular telephone calls are made by the cellular bandwidth thieves – many of which are made from stolen PINS and/or cellular telephones. Again, an identification of the legitimate ownership of the cellular telephones would prevent cellular telephone thieves from stealing the bandwidth. A reliable method of authenticating legitimate owner of an ATM card would greatly reduce ATM related fraud worth approximately $3 billion annually [6]. Solutions to common image processing attacks are found to be abundant and are generally considered easy. On the other hand, geometric distortion attacks are found to be more challenging as it causes synchronization error that can disable the detector. A positive method of identifying the rightful check payee would also reduce billions of dollars that are misappropriated through fraudulent encashment of checks each year. A method of positive authentication of each system login would eliminate illegal break-ins into traditionally secure (even federal government) computers. The United States Immigration and Naturalization service stipulates that it could each day detect/deter about 3,000 illegal immigrants crossing the Mexican border without delaying legitimate persons entering the United States if it had a quick way of establishing positive personal identification. These solutions are mainly using three schemes, namely, transform-based scheme (Lin *et al*., 2001) [12], the pilot-based scheme (Pereira and Pun, 2000)[15], and the feature-based scheme (Bas *et al*., 2002[3]; Tang and Hang, 2003[20]; Seo and Yii, 2004[18]; Lee *et al*., 2006[10]). The transform-based scheme embeds a fingerprint in affine-

invariant domain, while the pilot based scheme embeds an ownership and a redundant as a pilot signal for resynchronization. Feature based schemes use an invariant point extracted from an image to insert an ownership fingerprint (Licks and Jordon, 2005), [11]. In this paper, a feature-based finger identification algorithm using affine transform is proposed, and the purpose of content authentication is also achieved. A smoothly flowing pattern formed by alternating crests (ridges) and troughs (valleys) on the palmar aspect of hand is called a palmprint. Formation of a palmprint depends on the initial conditions of the embryonic mesoderm from which they develop. The pattern on pulp of each terminal phalanx is considered as an individual pattern and is commonly referred to as a fingerprint (see, Figure 1). A fingerprint is believed to be unique to each person (and each finger)2. Fingerprints of even identical twins are different. Irrespective of the technique or method used, the main objective of all these techniques is to produce a secure technique which does not degrade the quality of the cover image and reduce recognition accuracy. Several techniques exist for the protection of biometric data. The most commonly used techniques are Wavelets (Zebbiche *et al*., 2006), [22], Fourier Transformation (Ahmed and Moskowitz, 2005), [2], Discrete Cosine Transformation (Hui *et al*., 2008), [7], etc.

II. Fingerprint As A Biometric Method

Like many aspects of digital signal and image processing, fingerprinting schemes fall into two categories: spatial domain and transform domain techniques [1 - 5]. This depends on whether the fingerprint is encoded by directly modifying pixels (such as simply flipping low-order bits of selected pixels) or by altering some frequency coefficients obtained by transforming the image in the frequency domain. Spatial domain techniques are simple to implement and usually require a lower computational cost. However, such methods tend to be less robust to tampering than methods that place the fingerprint in the transform domain [6], [14], [15]. Fingerprints are one of the most mature biometric technologies and are considered legitimate proofs of evidence in courts of law all over the world. Fingerprints are, therefore, used in forensic divisions worldwide for criminal investigations. More recently, an increasing number of civilian and commercial applications are either using or actively considering to use fingerprint-based identification because of a better understanding of fingerprints as well as demonstrated matching performance than any other existing biometric technology. These include the following: (i) By transforming spatial data into another domain, statistical independence between pixels and high-energy compaction is obtained; (ii) the fingerprint is irregularly distributed over the entire

spatial image upon an inverse transformation, which makes it more difficult for attackers to extract and/or decode a fingerprint; (iii) it is possible to provide markers according to the perceptual significance of different transform domain components In the early 20th century, fingerprint identification was formally accepted as a valid personal identification method by law enforcement agencies and became a standard procedure in forensics [23]. Fingerprint identification agencies were setup worldwide and criminal fingerprint databases were established [23]. With the advent of live scan fingerprinting and availability of cheap fingerprint sensors, fingerprints are increasingly used in government and commercial applications for positive person identification. In addition, transform domain methods can hide information in significant areas of a cover text which makes them more robust to attacks and distortion while remaining visually imperceptible [10], [12], [13]. Cropping, for example, may seriously distort any spatially based fingerprint but is less likely to affect a transform based scheme because fingerprints applied in a transform domain are dispersed over the entire spatial domain so that upon inverse transformation, at least part of the fingerprint may be recovered. Lossy compression is an operation that usually eliminates perceptually unimportant components of an image and most processing of this type takes place in a transform domain. Thus, matching the transform with a compression transform can result in an improved performance (i.e. DCT for JPEG, Wavelet for JPEG-2000). Further, the characteristics of the Human Visual System (HVS) can be fully exploited in a transform domain, e.g. [13], [14].

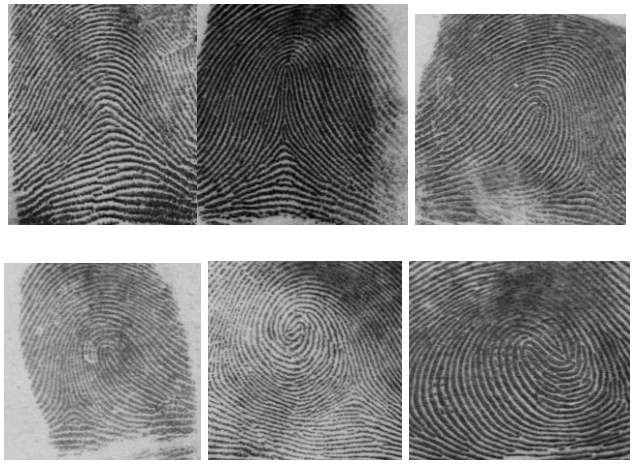

Figure 1: Fingerprints and a fingerprint classification schema involving six categories: (a) arch, (b) tented arch, (c) right loop, (d) left loop, (e) whorl, and (f) twin loop.

Critical points in a fingerprint, called core and delta, are marked as squares and triangles. Note that an arch does not have a delta or a core. One of the two deltas in (e) and both the deltas in (f) are not imaged. A sample minutiae ridge ending

(o) and ridge bifurcation (X) is illustrated in (e). Each image is 512 X 512 with 256 grey levels and is scanned at 512dpi resolution. All features points were manually extracted by one of the authors. With transform domain fingerprinting, the original host data is transformed to produce a matrix of 'coefficients'. These coefficients are then perturbed by a small amount in one of several possible ways in order to represent the fingerprint. Coefficient selection is based on 'perceptual significance' and/or 'energy significance'. When the fingerprinted image is compressed or modified by any image processing operation, noise is added to the already perturbed coefficients. Private retrieval operations involve subtracting the coefficients associated with the fingerprinted image from those of the original image to obtain the noise perturbation. The fingerprint is then estimated from the noisy data as best as possible. The most difficult problem associated with 'blind-mode' fingerprint detection (in which the host image is not available) in the frequency domain is to identify the coefficients used for fingerprinting. Embedding can be undertaken using quantization (thresholding) or image fusion, for example, but in either case, most algorithms consider the HVS to minimize perceptibility. The aim is to place as much information in the fingerprint as possible such that it is most robust to an attack but least noticeable. Most schemes operate directly on the components of some transform of the 'cover image' such as the Discrete Cosine Transform (DCT), Discrete Wavelet Transforms (DWT) and the Discrete Fourier Transform (DFT) [25], [26] [27]. In general, the HVS is not sensitive to small changes in edges and texture but very sensitive to small changes in the smoothness of an image [28], [29]. In 'flat' featureless portions of the image, information is associated with the lowest frequency components of the image spectrum, while, in a highly textured image, the information is concentrated in the high frequency components. The HVS is more sensitive to lower frequency than high frequency (visual) information. [1], [7], [8], [9]. Taking this into account, the following points are relevant to digital image fingerprinting in the frequency domain: (i) A fingerprint should ideally be embedded in the higher frequency range of an image in order to achieve better perceptual invisibility but only on the understanding that high frequency components can be distorted or deleted after attacks such as lossy compression, re-sampling or scanning, for example; (ii) in order to prevent the fingerprint from being attacked, it is often necessary to embed it into the lower frequency region of the spectrum, which cannot be attacked without compromising the image given that the HVS is more sensitive in this region; (iii) given points (i) and (ii), in order to embed a fingerprint in an image optimally (i.e. so that it can survive most attacks), a reasonable tradeoff is to embed a fingerprint into the intermediate frequency range of the image [10], [11], [12], [13].

III. Existing Work

The challenge in the case of image authentication is that in many cases images need to be subjected to non malicious operations like compression, so the authentication techniques need to be compression tolerant. IMAGE authentication techniques have recently gained great attention due to their importance for a large number of multimedia applications. Digital images are increasingly transmitted over non-secure channels such as the Internet. An image authentication system that is tolerant to JPEG lossy compression operations. An encrypted feature vector extracted from the image DCT coefficients is embedded redundantly and invisibly in the marked image. On the receiver side, the feature vector from the received image is derived again and compared against the extracted fingerprint to verify the image authenticity. This scheme is robust against JPEG compression up to a maximum compression of approximately 80%, but sensitive to malicious attacks such as cutting and pasting.

IV. Technique Outline

This paper aims at providing a fingerprinting technique for the copyright protection problem of color frontal facial images with uniform background based on the selection of certain robust facial features for fingerprint embedding.

• *Feature selection*: This stage is concerned with the preprocessing that is necessary to extract the spatial image characteristics needed for the fingerprint embedding/detection stage.

– Image segmentation: In this step, a skin-tone color segmentation technique is used that operates on the HSV color space, by selecting certain value ranges for the chrominance and luminance components.

– Feature detection: The resulting facial region is approximated by an ellipse, by means of a properly chosen neural network. Afterwards, the eyes and the center of the mouth are being searched for inside this ellipse, by trying to match them with appropriate simple geometrical templates. These three reference points define a rectangular area of certain dimensions, center and orientation. These parameters are finally used as input parameters for fingerprint embedding and detection.

• Fingerprint embedding/detection:

– Chaotic fingerprint embedding: A chaotic fingerprint that is constructed by Peano scanning of an one-dimensional (1-D) chaotic trajectory is embedded [9] according to the geometric parameters produced in the previous stage. The fingerprint is embedded on a rectangle corresponding to the facial image region of the previous stage.

– Chaotic fingerprint detection: A fingerprint detector based on the correlation of a fingerprint template with the possibly fingerprinted and processed image is proposed. This detector acts on a rectangle defined on the fingerprinted image in the same way as in the original one. Consequently, the robustness of the localization of the spatial features after several attacks on the fingerprinted image ensures the robustness of the detection process. In this way, only small local searches in the geometric parameter space are required to find the correct position of the embedded fingerprint.

V. Embedding And Extraction Algorithms

After the feature extraction process, the fingerprints for copyright protection and authentication are embedded into the cover image (Figure 1).

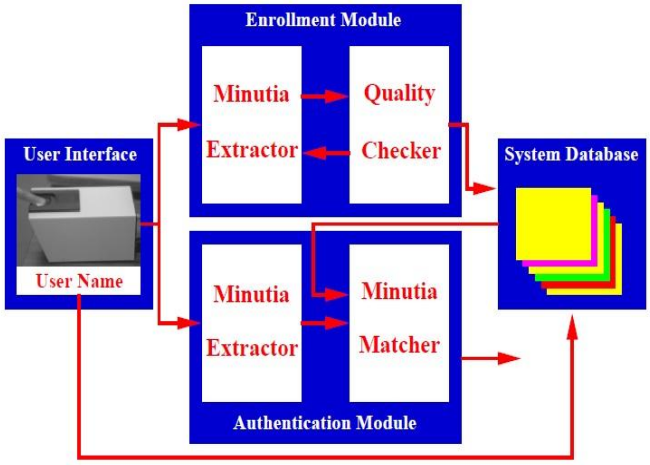

Figure 2: Architecture of an automatic identity authentication system.

Figure 1. Fingerprint Embedding Process.

At first, the feature points of an image are obtained by using the Hessian-Affine detector explained in the previous section. Moreover, the robust characteristic regions are chosen by the region selection. Then the following procedure is divided into two parts: the copyright insertion and the authentic insertion. The copyright insertion is mainly embedding the copyright fingerprint into the selected regions, and the fragile fingerprint is embedded into the remainder regions by the authentic insertion. Many feature points and characteristic regions are obtained after the feature detector. However, some of the feature points are useless and redundant because of the weakness of a region and the overlap between the regions. At first, the region selection removes over large or small regions, because a big or small characteristic region will be vulnerable if the local geometric transform is applied. All the regions whose characteristic scale is below 2 or above 12 are removed. Moreover, the region with smaller second derivative test discriminated is also removed when there are regions overlapped with each other. An image has been divided into two parts after the region selection, the

selected characteristic regions and the remainder regions. The first regions are processed by the copyright insertion, and the others are processed by the authentic insertion. Finally, the copyright and authentic regions to perform a fingerprinted image are combined and thus the fingerprinted image achieves copyright protection and content authentication simultaneously. In the fingerprint detection / extraction algorithm, once the characteristic regions are selected, the copyright detection and the authentic detection are initially used to detect the copyright fingerprint and the fragile fingerprint, respectively. The process is presented in figure 4.

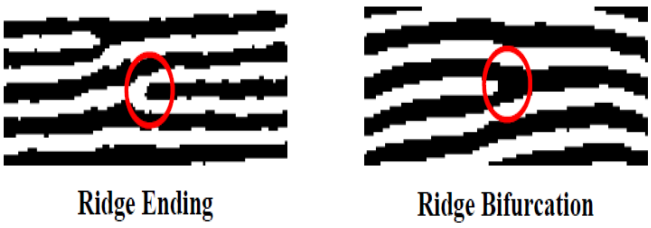

Figure 4: Ridge ending and ridge bifurcation.

Figure 4. The Detection Procedure.

Therefore, the copyright and the authentication of an image are determined according to the two kinds of the extracted fingerprints. A detected error is called false-alarm when there is no fingerprint embedded but detected having one. For an unfingerprinted image an extracted bit is treated as independent random variable with probability 0.5. The probability of success detection for a characteristic region (PSP-region) is calculated using Equation --- based on the Bernoulli trials.

$$P_{SP-region} = \sum_{i=n-T}^{n} \binom{n}{i} \cdot (0.5)^i \cdot (0.5)^{n-i}$$

Where *T* indicates the predefined threshold, and the parameters *i* is the number of the matching bits and *n* is the length of fingerprint bits. A fingerprint is said to exist if there are at least *m* regions detected. Therefore, the false alarm probability (*PSP-image*) of an image can be given as:

$$P_{SP-image} = \sum_{j=m}^{N} \binom{N}{j} \cdot (P_{SP-region})^j \cdot (1 - P_{SP-region})^{N-j}$$

where N are total regions found in an image, and j is the numbers of matching regions. The procedures for embedding the copyright and authentication fingerprint as well as extraction procedure used in this paper is adopted from Tsai *et al.*, 2007.

VI. Preventative Work

A.K.Jain and his research team primarily proposed digital fingerprinting. Jain and Umut [5] proposed multimedia content protection framework that is based on biometric data of the users. M.Vasta[6] presented a novel biometric fingerprinting algorithm for improving the recognition accuracy and protecting the face and fingerprint images from tampering. He made use of multi resolution DWT to embed face image in a finger print image. V-Support Vector Machine is exploited to enhance the quality of the extracted face image. Low etc al. [4] proposed to adaptively fuse Least Significant Bit (LSB) and Discrete Wavelet Transform (DWT)-based approaches into a unison framework, which to be known as LSBDWT scheme. The performance of LSB-DWT scheme is validated against simulated frequency and geometric attacks. Namboodiri, Jain [9] presented an LSB-based biometric fingerprinting scheme where a digital document was spatially fingerprinted with online handwritten signature. Kundur and Hatzinakos [10] were the pioneers in suggesting a fingerprinting model using biorthogonal wavelets based on embedding a fingerprint in detail wavelet coefficients of the host image. The model proposed was robust against numerous signal distortions, however it was non-blind. Yang [11] in his paper simulates under a spread-spectrum fingerprinting framework where a Gaussian distributed fingerprint is injected into the largest wavelet coefficients to find the best biorthogonal wavelet filter for multi resolution image fingerprinting. The performance of seven integer biorthogonal wavelet bases is evaluated and it is observed that the 917-F wavelet provides a substantial edge‟ when all detail sub bands are eligible for fingerprinting. The effect of using even-length and odd length biorthogonal wavelets for fingerprinting have been discussed in [12] and [13] respectively. Both these techniques were robust against several attacks, but were presented for the sake of detecting the presence of a fingerprint not for extracting it.

VII. Proposed Scheme

Signature is a behavioral biometric that is developed over the course of a person’s lifetime. Many people are very accustomed to the process of signing their name and having it matched for authentication. This process has been in practice for centuries and is well accepted among the general public to protect confidential information. The use of signature is prevalent in the legal, banking, and commercial domains. Each person has a unique handwritten signature. The way a person signs their name or writes a letter can be used to prove a person's identity. These important traits of the handwritten signature is a motivation in embedding it as a fingerprint in an image.

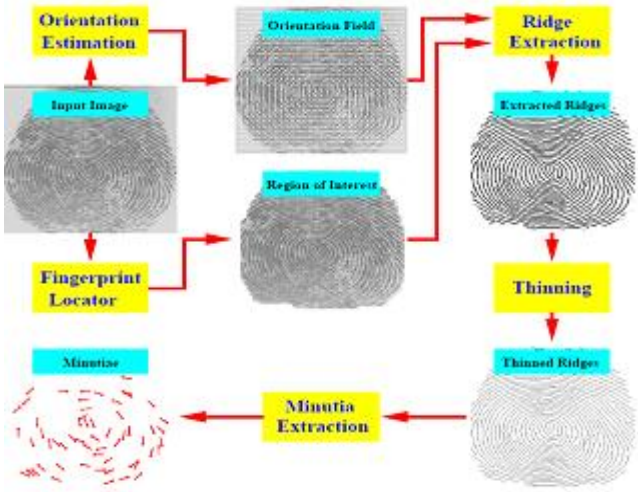

Figure 6: Flowchart of the minutiae extraction algorithm [18].

This section describes the proposed fingerprinting method which performs a 2-level DWT on the host image using biorthogonal wavelet. An offline hand written signature from the user is preprocessed and converted into a binary bit string before embedding. The proposed scheme is carried out in four phases, fingerprint preparation from signature image, the signature embedding phase, the signature recovery phase and feature extraction and template matching phase. Figure 1 shows the block diagram of proposed fingerprinting scheme.

1. Fingerprint Preparation

A binary bit string of the signature image selected by the user for embedding is generated. The signature image is converted to a 1-D binary string through vector division with values ranging between 0 and 1 only. This is essential as fingerprinting will be done based on these two values only.

2. Fingerprint Embedding

The following steps are followed for the fingerprint embedding. 1. A 2-level 2D DWT decomposition using biorthogonal filters is performed on the input image to generate the output image X. The host image is first subjected to the first level DWT to obtain one approximate (LL1) and three detailed (HL1, LH1 and HH1) sub-bands. The DWT approximate band represents the coarse region with significant low frequency coefficients. To obtain the next coarser domain, LL1 is further sub-sampled. In contrast, the detailed coefficients denote the finest domain that is occupied by middle and high frequency coefficients. Therefore, additional sub-sampling of the detailed coefficients is prohibited. In the proposed method, the sub-image was subdivided into 2-level DWT decomposition as shown in Figure 2. The detailed coefficients (HL2, LH2 and HH2) hence obtained are used for the process of embedding fingerprint. A secret key is used to generate

pseudorandom sequences to ensure confidentiality and these sequences are used as a fingerprint depending upon the signature bit.

2. Generate number of PN sequences having mean 0 and variance 1 and the same dimension and structure of the image X using a secret key. Number of PN sequence generated will be equal to number of bands used for embedding. For embedding in HL2 band only, one PN sequence is generated, for embedding in HL2 and LH2 bands, two PN sequences are generated while for embedding in all the three bands, three PN sequences are generated.

3. To effectively differentiate between fingerprint bit "0" and "1", whenever the signature bit is zero, these pseudo-random sequences, are inserted into the horizontal detailed wavelet coefficients (or into HL2 and LH2 or in to all three bands) whenever the fingerprint bit is zero else the wavelet coefficients are left untouched. A large α (embedding factor) might be used to optimize the fingerprint robustness at the expense of host fidelity. Hence, a fine trade-off should be experimentally determined to strike a proper balance between the fingerprint imperceptibility and the fingerprint robustness. In proposed scheme, value of α is set in the range of 0.5 to 0.7 to obtain a balanced mix of robustness and fidelity.

<table>
<tr><td>LL2</td><td>HL2</td><td rowspan="2">HL1</td></tr>
<tr><td>LH2</td><td>HH2</td></tr>
<tr><td colspan="2">LH1</td><td>HH1</td></tr>
</table>

Figure 2. Second level decomposition LL represents the approximation sub-band, HL represents the horizontal sub-band, LH represents the vertical, and HH represents diagonal sub-band.

4. The pseudo-random sequence thus generated during each pass is used to update the horizontal detailed coefficients using Cox"s [27] algorithm only when the fingerprint bit is 0, in case it is one , the coefficients are unaltered.

$$HL2=HL2+\alpha PN\_sequence\_1 \quad (5)$$

If fingerprint is embedded in both bands then

$$LH2=LH2+\alpha PN\_sequence\_2 \quad (6)$$

If it is embedded in all three bands then

$$HH2=HH2+\alpha PN\_sequence\_3 \quad (7)$$

5. Finally, the fingerprinted image I' is reconstructed using the inverse DWT

3. Fingerprint extraction

1. The key shared between the embedder and the authenticator is used to re-generate pseudo-random sequences. Number of sequences generated equal to number of bands being used for embedding .
2. Another sequence „W‟ consisting of only 1‟s equal to the length of the original fingerprint is also generated which is further used to generate/reconstruct the fingerprint.
3. The 2-level Biorthogonal DWT of the fingerprinted image is performed to obtain the detailed coefficient. Being a blind fingerprinting technique, for fingerprint recovery, original cover image is not required in this approach.
4. For each PN sequence generated, the correlation between this sequence and the horizontal detailed coefficient is calculated and stored in a 1-D sequence equal to the length of the fingerprint.

correlation_HL2 (i)=corr2(HL2, PN_sequence_1) (8)

If fingerprint is embedded in both bands then

correlation_LH2 (i)=corr2(LH2, PN_sequence_2) (9)

If fingerprint is embedded in all three bands then

correlation_HH2 (i)=corr2(HH2, PN_sequence_3) (10)

5. In case the fingerprint is embedded in two or three bands, then finally the average of correlation sequences is found out. The standard deviation of this correlation sequence thus formed is calculated and then compared to each value of the correlation sequence to decide the fingerprint bit.
6. The decision for updating the fingerprint bit is taken depending upon the value obtained in the step above.

If correlation[i] > std(x)

set corresponding bit in „W‟ to Zero

else

that particular bit is left unaltered.

7. The original signature image is reconstructed by reshaping the sequence „W‟ thus obtained from step 6.

4. Template Matching Based Authentication

The signature pattern thus reconstructed is authenticated using template matching. The features of the entire signature database are extracted using the steps mentioned in the latter part of this section. The same steps are used to extract the

features of the recovered signature and then using the euclidean distance as a measure, the features of recovered signature are matched with the features of signature from the database. Feature Vector Generation The flowchart in Figure 3 shows the process of feature vector generation. It consists of mainly two steps, preprocessing and feature extraction. Preprocessing is done to the signature images from data base so as to prepare it for the process of feature extraction and to ensure that all the signature images are of the same dimensions so that it is easier and convenient to extract the features.Preprocessing is carried out in the following three steps. Median Filtering: Generally, digital image might contain speckles, smears, scratches or other forms of unwanted noise that might thwart feature extraction. Thus, median filtering is used to eliminate the existing noises. Binarization: The process by which the image is converted into black and white is called binarization. For a signature image X having dimensions m and n, the following equation is used to find out the level of Binarization [21].

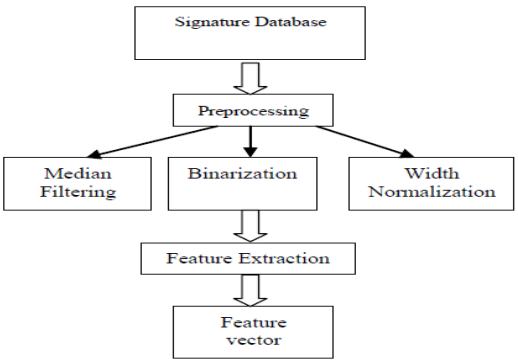

Figure 3 Feature Vector Generation Flowchart

$$P = (\Sigma\Sigma X(i,j))/(m*n)) \quad (11)$$

Where P = Average value of all pixels in the image.

Feature Extraction

Figure 4 depicts the process of feature extraction from the normalized signature images using Hough Transform and Principal component analysis.

VIII. Experimental Results

The two models proposed with Hessian and Gillies' were tested with three images namely, Lena, Baboon and Pepper. The cover image, the copyright image and authentication images used are given in Figure 3-. The images selected were grey-scale images of size 256 x 256 but the algorithm works for 512 x 512 also. The various attacks tested are Rotate 1_, Rotate 5_, Rotate 45_, Rotation 1_ and Scale, Rotation 45_ and Scale, Crop 10 %, Crop 25%, Crop 50%., Scale 50%,

Scale 90%, Scale 110%, Median 2x2, Median 3x3, Median 4X4, Gaussian 3x3, JPEG with quality factor 20, JPEG with quality factor 40, JPEG with quality factor 60 and JPEG with quality factor 80.Which are numbered from 1 to 19 respectively in Table 1.

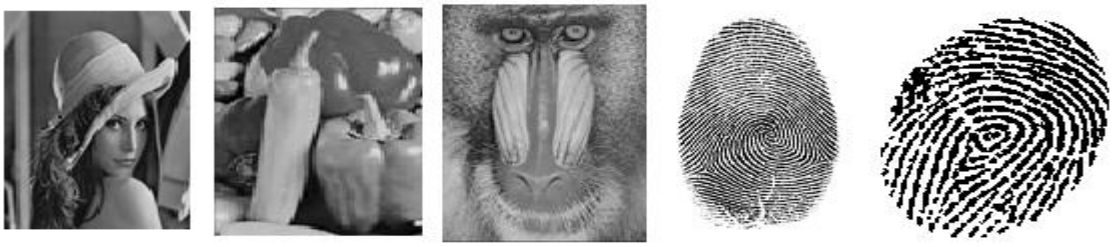

Figure 3. Cover, Copyright and Recognition Images.

The system was tested with two performance metrics, namely, number of feature points detected and time taken for embedding and extracting the fingerprint.

A Survey of Copy-Move Forgery Detection Techniques

Copy-move forgery is a specific type of image tampering where a part of the image is copied and pasted on another part generally to conceal unwanted portions of the image. Hence, the goal in detection of copy-move forgeries is to detect image areas that are same or extremely similar. It reviews several methods to achieve this goal. These methods in general use block-matching procedures, which first divide the image into overlapping blocks and extract features from each block, assuming similar blocks will yield similar features. Later, a matching step takes place where the aim is to find the duplicated blocks based on their feature vectors. A forgery detection decision is made only if similar features are detected within the same distance of features associated to connected blocks. Maliciously manipulate, and tamper digital images without leaving any obvious clues became very easy with the widely available, easy to use and extremely powerful digital image processing tools such as Photoshop and Freehand. It considers a specific type of image forgery where a part of the image is copied and pasted on another part of the same image mostly to cover an important object. An example for this type of forgery can be seen in Figure.2.6, where a group of soldiers are duplicated to cover President George W. Bush. This process can be done without any modifications on the duplicated regions. As a result, the tampered region would exhibit the same characteristics as the rest of the image which makes it hard to identify using the tools that are designed to detect the anomalies in the image. Hence, to detect copy-move forgeries, it needs techniques that can detect the image regions which occur more than once in the image. A good copy-move forgery technique should

detect the duplicated image regions, without getting affected by the slight modifications and/or operations such as noise addition, and compression. To accomplish this task several copy-move forgery detection techniques have been used.

Figure 2.6. Left is manipulated right is the original images.

IX. Performance Evaluation: In order to evaluate and compare the performance of the copy move forgery detection methods as shown in Table 2.2, it picked three methods where DCT features, PCA features, and FMT features are used and implemented these methods. As block size, b = 16. It was assumed that the duplicated region would be at least 32x32. Considering the blocks which would be affected by the image processing operations chose the threshold value as 150. While comparing these methods, it uses lexicographically searching in matching step.

Table2.2. Performance Results

Manipulation type	FMT	DCT	PCA
JPEG	20	40	50
Rotation	10°	10°	0°
Scaling	10%	10%	0%

The copy-move forgery detection is one of the emerging problems in the field of digital image forensics. Many techniques have been proposed to address this problem. One of the biggest issues these techniques had to deal with was, being able to detect the duplicated image regions without getting affected by the common image processing operations, e.g. compression, noise addition, rotation.

Conclusion: Fingerprinting techniques are increased used in biometric security systems for authentication requirements and they use biometric characteristics such as face, voiceprint, fingerprint, etc. Out of these, iris image is considered to be more reliable for personal authentication. They are considered good choice because of two very important characteristics, its uniqueness and permanency. The results obtained prove that both the algorithms withstand to attacks.

Future research directions are to convert the same algorithms for color images and to improve the accuracy of location to insert the fingerprint by considering a better characteristic region selector.

References

1. Lin,C.(2000) Fingerprinting and Digital Signature Techniques for Multimedia Authentication and Copyright Protection, PhD Thesis, Columbia University, 2000.
2. Ahmed, F. and Moskowitz, I.S. (2005) Composite Signature Based Fingerprinting for Fingerprint Authentication, ACM Multimedia and Security Workshop, New York, Pp. 1-8.
3. Bas, P., Chassery, J.M. and Macq, B. (2002) Geometrically Invariant Fingerprinting Using Feature Points, IEEE Trans. IP, Vol.11, No.9, Pp.1014-1028.
4. Daugman J and Downing C (2001) Epigenetic randomness, complexity, and singularity of human iris patterns, Proceedings of the Royal Society, B, 268, Biological Sciences, Pp 1737 - 1740.
5. Gilles, S. (1998) Robust description and matching of images, PhD Thesis,University of Oxford.
6. Harris, C. and Stephens, M. (1988) A combined corner and edge detector, Alvey Vision Conference, Pp. 147–151.
7. Hui, K., Jing, L., Xiao-dong, Z. and Xiao-xu, Z. (2008) Study on Implementation of a Fingerprint Fingerprint, International Conference on Computer Science and Software Engineering (CSSE), Vol. 3, Pp.725-728.
8. Inaba, H. and Kasao, M. (2000) Notes on Alteration Attack for Digital Fingerprint, Technical report of IEICE, IT99-103.
9. Kadir, T. and Brady, M.(2001) Saliency, scale and image description, International Journal of Computer Vision, Pp. 83–105.
10. Lee, H.Y., Kim, H. and Lee, H.K. (2006) Robust image fingerprinting using local invariant features, Journal SPIE, Optical Engineering, Vol.45, No.3, Pp. 1-7.
11. Licks, V.and Jordan, R. (2005) Geometric Attacks on Image Fingerprinting Systems, IEEE Multi-Media, Vol.12, No.3, Pp.68-78.
12. Lin, C.Y., Wu, M., Bloom, J.A., Cox, I.J., Miller, M.L. and Lui,Y.M.(2001) Rotation, scale and translation resilient fingerprinting for image, IEEE Trans.Image Processing, Vol.10, No.5, Pp.767-782.

13. Lowe, D. (2004) Distinctive image features from scale-invariant keypoints, International Journal of Computer Vision, Vol. 2, Pp.91–110.
14. Mikolajczyk, K. and Schmid, C. (2004) Scale and affine invariant interest point detectors, International Journal of Computer Vision, Pp. 63–86.
15. Pereira, S. and Pun, T. (2000) Robust template matching for affine resistant image fingerprints, IEEE Trans.Image Processing, Vol.9, No.6, Pp. 1123-1129.
16. Pereira, S. and Pun. T. (1999) Fast robust template matching for affine resistant image fingerprinting, International Workshop on Information Hiding, vol. LNCS 1768, Pp. 200-210.
17. Ratha, N.K., Connell, J.H. and Bolle, R.M. (2000) Secure data hiding in wavelet compressed fingerprint images, Proc.ACM Multimedia 2000 Workshops, Los Angeles, CA, Pp. 127-130
18. A. Jain, L. Hong, S. Pankanti, and R. Bolle, On-line identity-authentication system using fingerprints, Proceedings of IEEE (Special Issue on Automated Biometrics), vol. 85, pp. 1365– 1388, September 1997.
19. A. K. Jain, S. Prabhakar, and L. Hong, A Multichannel Approach to Fingerprint Classification, Proc. of Indian Conference on Computer Vision, Graphics, and Image Processing (ICVGIP'98), New Delhi, India, December 21-23, 1998.
20. T. Kamei and M. Mizoguchi. Image filter design for fingerprint enhancement. In Proc. ISCV'95, pages 109–114, Coral Gables, FL, 1995. 30
21. K. Karu and A. K. Jain, Fingerprint Classification, Pattern Recognition, Vol. 29, No. 3, pp.389-404, 1996.
22. M. Kawagoe and A. Tojo, Fingerprint Pattern Classification, Pattern Recognition, Vol. 17,No. 3, pp. 295-303, 1984.
23. H. C. Lee and R. E. Gaensslen, Advances in Fingerprint Technology, Elsevier, New York,1991.
24. D. Maio, D. Maltoni, Direct Gray-Scale Minutiae Detection in Fingerprints, IEEE Trans. Pattern Anal. Machine Intell., Vol. 19, No. 1, pp. 27-40, 1997.
25. B. M. Mehtre and B. Chatterjee, Segmentation of fingerprint images – A composite method, Pattern Recognition, Vol. 22, No. 4, pp. 381–385, 1989.
26. N.J. Naccache and R. Shinghal, An Investigation into the Skeletonization Approach of Hilditch, Pattern Recognition Journal, Vol. 17, No. 3, pp. 279-284, 1984.