Available online at www.sciencedirect.com

ScienceDirect

Procedia Technology 10 (2013) 172 – 183

Procedia Technology

International Conference on Computational Intelligence: Modeling Techniques and Applications (CIMTA) 2013

A novel EMD based watermarking of fingerprint biometric using GEP

Anil Kumar Shaw[a], Swanirbhar Majumder[b*], Souvik Sarkar[c], Subir Kumar Sarkar[d]

[a]*NIELIT(formerly DOEACC Society), Itanagar, Arunachal Pradesh-791111, India*
[b]*Department of ECE, NERIST, Deemed University, Itanagar, Arunachal Pradesh-791109, India.*
[c]*IBM, Hydrabad, Hydrabad, Andhra Pradesh-500001, India.*
[d]*Departmant of ETCE, Jadavpur University, Kolkata, West Bengal-700032, India*

Abstract

Watermarking with biometrics has been proposed as a line of defense in the protection of IPR and DRM. Robust watermarking of biometric information of the user in the host data may be used for this purpose. Fingerprints are the most popular and non-invasive biometric data used most widely. Here a process of embedding fingerprints data using a novel method of empirical mode decomposition (EMD) and gene expression programming (GEP) together is provided. The watermarking algorithm provided uses singular value decomposition (SVD) and lifting based discrete wavelet transform (DWT). The method provided is secure, robust and imperceptible form of watermarking. This watermarking technique has the advantage of using SVD and lifting based DWT which do not involve convolution thereby being easily implementable on hardware.

Selection and peer-review under responsibility of the University of Kalyani, Department of Computer Science & Engineering

Keywords: Watermarking; biometrics; fingerprint; singular value decomposition (SVD); empirical mode decomposition (EMD); gene expression programming (GEP); lifting based discrete wavelet transform

* Corresponding author. Tel.: +919436229406.
E-mail address: swanirbhar@gmail.com.

Selection and peer-review under responsibility of the University of Kalyani, Department of Computer Science & Engineering
doi:10.1016/j.protcy.2013.12.350

1. Introduction

In this age of the tech-savvy world digital watermarking is a very important technique, for the copyright protection and security of multimedia data. If the logos, which are commonly used in watermarking are replaced by biometric data the security intensity would be enhanced. With the inclusion of biometrics for watermarking schemes, the concept of "something you are" is included in the watermark and/or cover image [1-6]. Here fingerprint has been used as it is the most popular, easily extractable and implementable biometrics with substantial amount of security [1].

The finger print verification competition (FVC) 2004 databases has been used here for fingerprint [3]. These images require initial preprocessing techniques. There is separate algorithm using empirical mode decomposition (EMD) for fingerprint feature extraction and matching [7] [8]. Unlike standard biometric algorithms here too much of complexity cannot be employed. It is because the watermarking technology needs to be employed along with the biometrics.

Biometric identification is generally preferred over traditional methods such as passwords, smart-cards, etc., because its information is virtually impossible to steal as it is "something you are." A number of biometric characteristics are being used in various applications as Universality, Uniqueness, Measurability, Performance, Acceptability, and Circumvention. Watermarking of biometric data, may be in either way. That is, it might be a biometric image template being watermarked for its authenticity or a host/carrier image being watermarked by the user's or author's biometric for copyright issues. A few different techniques of either type that have been employed concerning a few established works are hereby discussed [1] [3] [9] [10].

Rao *et.al.* have discussed a method for copyright protection of digital images by watermarking the images with the fingerprint features of the author/owner. Here the minutiae points were extracted from the fingerprint and their coordinates are represented as a matrix to utilize them as the watermark [11]. The transform domain used is a hybrid form of the discrete cosine transform (DCT) and SVD. This is done by extracting the coordinates of the minutiae points from the watermarked image and compared with those extracted from the fingerprint of the person claiming the ownership. Similarly for the issues on privacy, security and legal significance of text documents, Lam et. al. proposed a similar scheme as above with fingerprint as the secret key [12]. Their scheme ensures the genuineness and integrity of the text document by encrypting the digital biometric fingerprint of the signatories. The fingerprint watermark message was extracted after decryption, based on 'odd' and 'even' pixels in each block of the embedded document. Dutta et.al. did a similar work on audio data with iris biometric instead of the fingerprint [13]. They term the pseudorandom sequences, the generation of which is based on iris image templates as the bio-keys, and watermark the audio signal for distinct identification. And on the lines of fingerprint as in the work of Rao et. al. [11] a similar work using wavelets have been done using iris biometric [14].

Watermarking of using biometrics data method may also be undergone other way around with the biometric being watermarked with any particular data or even another biometric. Naik et. al. provided blind digital watermarking algorithm using mapping technique [15]. The cover image used is fingerprint biometric and the watermark is a facial image. The scheme in discussion is blind and there by requires no addition data for logo extraction. For threats designed to extract information about the original biometric data of any person from any stored database system, as well as the authentication of the entire system, Islam et.al, had proposed a scheme to address privacy and security [16]. Their system trekked through insecure internet/intranet in communication lines/systems for security against attacks and eavesdropping.

For high security to both hidden data i.e., fingerprint minutiae that has to be transmitted and the host image i.e., fingerprint Zebbiche et al. provided a system [17]. Here the original unmarked fingerprint biometric is not required to extract the minutiae data. The method was essentially introduced by them to increase the security of fingerprint minutiae transmission as well as to protect the original raw fingerprint image. Mathivadhani et. al. [18] compared the other biometric watermarking techniques of Zebbiche et al. [19] and Vasta et al. [20], both based on Discrete Wavelet Transformation (DWT). They found that for the copyright protection of fingerprint biometric data using digital watermarking techniques, both provide adequate security to the data without degradation of visual quality.

Iris based biometrics have also been watermarked using affine parameters estimation (APE) by Li and Du [21]. Radon Transform has been used by them to determine the regular grid of points for estimation for iris images, which is used for the general affine transform determination and applied to the images. They improved the

Voloshynovskiy's methods and showed that this problem can be solved by Radon transform. Similarly, voice and iris based biometrics were combined together by Bartlow et.al. in a watermarking scheme [22]. The raw iris images in a secure centralized database were encoded with voice feature descriptors to provide an added authentication level and as a mechanism for origin of iris images' validation. Moreover, the system also helps in understanding the levels at which the watermarks could be compromised as well as implementation of a particular asymmetric watermarking framework.

Face and fingerprint based multimodal biometric based blind image watermarking, with hidden thumbnail feature vectors, through a two-stage integrity verification method for safe authentication of data was proposed by Kim et.al [23]. The basic idea is to use the face image thumbnail's feature vectors as the watermark pattern to be embedded into the raw fingerprint biometric images. It comprised of two stages. Firstly, the integrity for a fingerprint image is verified by deciding the validity of extracted thumbnail patterns. Secondly, based on one to one matching between thumbnail feature vectors extracted from a face image and the thumbnail one of the received face images' integrity is verified. All this is done to get a high detection rate of the forged biometric data and guarantee the security assurance.

In their work, the VLSI Design and CAD Laboratory of University of North Texas have presented a new approach and architecture in the framework of a digital camera, conceptualized as a "Secure Digital Camera (SDC)" [24], [25]. The SDC uses watermarking and encryption processes for image security and authentication. The Rijndael AES algorithm [26] and a DCT-based visible watermarking algorithm [27] were chosen for implementation in the camera. The proposed architectures were modeled, simulated and synthesized in Xilinx ISE. They included bar codes along with multimodal biometric comprising of iris, fingerprint and signature and mixed them up in a mixer to get a visible as well as an invisible watermark. Both watermarks are then applied on each individual image. Once implemented on field programmable gate array (FPGA) and tested, the system can very easily go for application specific integrated circuit (ASIC) or system on chip (SoC) implementation for real-time applications.

Here the algorithm used employs the hybrid SVD and lifting based DWT watermarking algorithm used in [2] using iris images of University of Bath. But the iris image template generated by CRC coding of the DC values of the iris image template via DCT. But instead of using the iris images the fingerprint images of FVC 2004 database have been used [3]. But the novelty in this work is in the method used in creating the fingerprint feature template to be watermarked.

2. Introduction

It is known that computers/system/any facility should be only accessed by legitimate users. To know if a user is legitimate or not, the system may be supplied with a username and a method of authentication. The most common way to identify a user is through a username or identification (ID). These often take the following forms: last name, last name with first initial, employee ID, etc. How a user authenticates depends on the authentication methods available. There are three main ways to authenticate an identity:

a) Something you know, like a password or pass phrase
b) Something you have, like a token.
c) Something you are, a measurable trait.

A biometric measures a particular individual's unique physical or behavioral characteristics to recognize or authenticate their identity. Common physical biometric are fingerprints; hand or palm geometry; and retina, facial or the iris. Behavioral characteristics include signature, voice, which also has a physical component, keystroke pattern, and gait. Biometrics is based on identification, which establishes a person based only on biometric measurements, i.e., 1: N matching algorithm and verification which involve confirming or denying a person's claimed identity, i.e., 1:1 matching algorithm [1].

Biometrics is characterized on the basis of the following features:

a) highly unique – so that the chance of any two people having the same characteristic will be minimal,
b) stable – so that the feature does not change over time, and
c) be easily captured – in order to provide the convenience to the user, and prevent misrepresentation of the feature.

Thus, a biometric is the most secure and convenient authentication tool. A few popular biometrics are as under.

But other than these, there are many more like keystroke dynamics, gait, tongue print, dental scan, etc [1] [4].

2.1. Fingerprint as Biometric

Started for prisoners' record, it involves taking an image of a person's fingertips and records its featured characteristics like whorls, arches, and loops along with the patterns of ridges, furrows, and minutiae. Fingerprint matching can be achieved in three ways.

a) Minutiae based
b) Correlation based
c) Ridge feature based

To capture the fingerprints different sensors are employed:

a) optical sensors that use a CCD.
b) CMOS image sensor;
c) solid state sensors (working based on capacitive, thermal, electric field or piezoelectric sensors);
d) Ultrasound sensors (working on echo graphic, where the sensor sends acoustic signals through the transmitter to the finger and captures the echo signals at the receiver)

Fingerprints are the most, user-friendly and widely biometric. Whereas Iris biometrics like fingerprints are to some extent a bit less non invasive and but more secure. It also comes second in popularity along with facial recognition. It has an added advantage that fingerprint scanners are very much robust unlike iris scanners. The consumers or the particular person whose biometric is to be analyzed too is very comfortable in providing his fingerprint. This is because it is easier to place a finger on the scanner for fingerprint compared to placing an eye in the infra-red (IR) iris camera. But Iris based biometrics has their own set of advantages starting from higher categorical uniqueness as well as being constant throughout the life of the person concerned. Moreover the dilation property of iris biometric, if included, enhances the security as the system can work till the person concerned is living. DNA, vein and retinal scan based biometrics are among the best but problem is that they are not very user-friendly. They can be used in individual cases but for group authentications it is not very much popular [1].

The performance of a fingerprint verification system highly depends on the situation in which it is used. Users may be well trained to use the system conscientiously but for situations like physical access control applications it might be otherwise. Fingerprints are affected if the users are cold, wet, or sweaty because of weather conditions, etc. People's impatience may lead to incorrect acceptance or rejection. Enrolment is another critical issue. If the enrolled fingerprints are not of high quality, system performance decreases significantly. Therefore, enough time has to be taken for the enrolment. Especially when the enrolment is unsupervised, feedback of the acquisition process is important. Users need to know whether they have to press harder or to place their fingers differently on the sensor.

Most verification systems use an ID card to store the claimed identity of a user. In this situation, achievement of an extremely low false acceptance rate (FAR) is not a critical issue. Impostor attempts occur only sporadically, since the impostor first has to get access to a valid ID card. If an attempt is made with a stolen ID card that has not been reported as missing, the fingerprint verification serves as an additional barrier. In such a case, an FAR level of 1% is satisfactory, while most algorithms offer an FAR of 10-3 or better.

2.2. EMD based Fingerprint biometric technology

A fingerprint is a pattern of curving line structures called ridges, where the skin has a higher profile than its surroundings, which are called the valleys. In most fingerprint images, the ridges are black and the valleys are white. Though it is not as secure as retinal scan or iris still it is the most widely used biometric. Many people may not feel comfortable to provide their iris/retinal data as they contain vital medical information and are a bit uncomfortable as well, whereas the fingerprint biometrics are very much user friendly in comparison.

A review on fingerprint classification methods can be found in [28]. Core and delta points are the main features used in rule-based approaches such as the one proposed by Kawagoe and Tojo [29]. In [30], ridges represented by B-spline curves were employed for the same purpose. A structural approach using partitioning of the orientation field into homogeneous regions has been proposed in [31] [32]. Prabhakar et al. [33] proposed a set of Gabor features showing promising results. In [34], Fitz et al. introduced frequency based features to perform classification.

Minutiae information based study presented a feature extraction method based on the position, location and orientation associated with minutiae points [35]. In a different study [36], genetic programming was used to learn a set of features for classification.

This study presents a comparative analysis of several different feature extraction methods for fingerprint classification. Due to all kinds of noise and distortions, fingerprints cannot be matched simply by taking the cross-correlation or the Euclidean distance of the gray scale images. This is solved to some extent by extracting features from the fingerprints that are more robust to the distortions. Commonly used features are:

a) Directional field (DF): It is defined as the local orientation of the ridge-valley structures. It describes the coarse structure, or basic shape, of a fingerprint and is calculated on a regular grid in the fingerprint.
b) Singular points (SPs): They are the discontinuities in the directional field. Two types of SP exist. A core is the uppermost point of the innermost curving ridge, and a delta is a point where three ridge flows meet. In some fingerprints, the SPs fall outside the image area.
c) Minutiae: They provide the details of the ridge-valley structures. Automatic fingerprint recognition systems use the two elementary types of minutiae that exist, being ridge endings and bifurcations. Sometimes composite types of minutiae such as lakes or short ridges are also used.

In fingerprint recognition system, the directional field is used for enhancement of the fingerprint together with the singular points for classification, while the minutiae are used for matching.

In the proposed algorithm, the fingerprint features are extracted from the fingerprint verification competition database announced by the Biometric Systems Lab (University of Bologna), the Pattern Recognition and Image Processing Laboratory (Michigan State University) and the Biometric Test Center (San Jose State University). This database was called FVC 2004[37]. Minutiae point like bifurcation and ending are obtained after performing a series of preprocessing steps, minutiae extraction and post processing as shown in Figure 1. The various steps in minutiae extraction are:

a) The preprocessing steps involving steps like image enhancement, histogram equalization and image binarization.
b) During minutiae extraction, the image is thinned and Minutiae points like bifurcation and ending is marked. Then the false minutiae are removed under post processing.
c) The coordinates of the minutiae points are used to extract the minutiae point intensities
d) Empirical mode decomposition (EMD) is applied on the intensities to obtain a set of intrinsic mode functions (IMFs) and the relevant residue.

The pre-decided particular IMF of minutiae point intensity is used as the watermark after being converted to binary code with CRC.

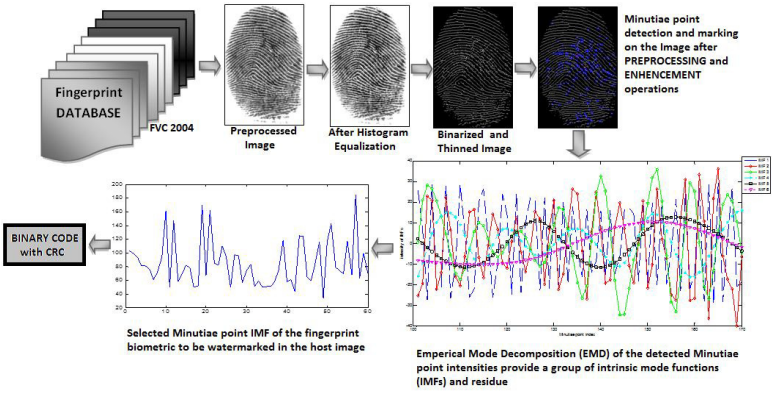


Fig. 1. EMD based Fingerprint biometric technology

The novel technique employed here is EMD [7][8]. EMD has mostly been employed in audio and speech, ECG, and other one dimensional signals. In the field of iris biometrics it has been used as in [38], but had not been used in fingerprint analysis as yet. The EMD method designed by N. E. Huang [8] for nonlinear and non-stationary signal

analysis is about decomposing any complicated data set to a finite and often small number of IMFs that admits well-behaved Hilbert transforms. This decomposition method is adaptive, and, therefore, highly efficient. Since the decomposition is based on the local characteristic time scale of the data, it is applicable to nonlinear and non-stationary processes.

Here the IMFs are to satisfy two different conditions. Firstly, in the whole data set, the number of extrema and number of zero crossings must either equal or differ at most by one. Secondly at any point, the mean value of the envelope defined by the local maxima and the envelope defined by the local minima is zero. In brief, the decomposition processing can be called sifting process. The goal of sifting is to subtract the large-scale features of the signal repeatedly until only the fine-scale features remain. The steps of the sifting are as follows:

a) Identify the extrema (maxima and minima) of the signal *x(t)*.
b) Find the upper envelope of the *x(t)* by passing a natural cubic spline through the maxima, and similarly, find the lower envelope of the minima.
c) Compute mean of the upper and lower envelopes and designate as *m(t)*.
d) Get an IMF candidate using the formula $h_i(t) = X(t) - m_i(t)$.
e) Check the weather properties $h_i(t)$ is an IMF. If $h_i(t)$ is not an IMF, repeat the procedure from step 1. If $h_i(t)$ is an IMF, then set $r = X(t) - h_i(t)$ and then $h_i(t) = c_i$

The procedure is repeated by sifting the residual signal. The sifting processing ends when the residue r satisfies a predefined stopping criterion. The $h_i(t)$ (i=1…..n) are being sorted in descending orders of frequency. Finally, the original *x(t)* can be reconstructed by a linear superposition:

$$X(t) = \sum_{i=1}^{n} c_i(t) + r_n(t) \tag{1}$$

where c_i is the i th IMF of the decomposed signal, and r is a residue.

2.3. GEP based standardization of the IMF

Genetic Algorithm (GA) [10] is the best known algorithm from the Evolutionary Algorithm (EA) class. In the conventional version, chromosomes represent as a fixed length binary string. Genetic Programming (GP) [39] in another version of GA, where chromosomes are represented as a LISP expression translated graphically into a tree. Candida Ferreira in 2001, motivated from biological evolution introduced and proposed version of the Evolutionary Algorithms, called Gene Expression Programming (GEP). It overcomes certain limitations of GA and GP by working with two elements, the chromosome and the expression tree. The chromosome is the encoder of the candidate solution which is then translated into an expression tree. GEP is an example of a full-fledged replicator/phenotype system where the chromosome /expression trees form a truly functional, indivisible whole [40]. That's why GEP is a big breakthrough in evolutionary computation, and it continuously is attracting more and more researcher attentions recently, especially in the areas of data mining. It should be noted that GEP chromosomes are multigenic. It encodes multiple expression trees or sub-programs, later on which can be structured into a much more complex program. Because of this, as like the DNA/protein system of life on Earth, the gene/tree system of GEP not only explores all the crannies and paths of the solution space but it has also the scope to explore sophisticated levels of organization.

Thus in short, Gene expression programming (GEP) is an evolutionary algorithm that creates computer programs or models. These computer programs are complex tree structures that learn and adapt by changing their sizes, shapes, and composition, much like a living organism. And like living organisms, the computer programs of GEP are also encoded in simple linear chromosomes of fixed length. GEP is a genotype-phenotype system, benefiting from a simple genome to keep and transmit the genetic information and a complex phenotype to explore the environment and adapt to it. Here GeneXpro software does that automatically to select the relevant IMF of the fingerprint. Thus, for each person, a standard IMF is chosen via GEP [41] [42]. The selected standard IMFs are seen to follow a particular type of pattern out here, based on which they can be differentiated. But if the IMFs of different persons' fingerprint for any one image are plotted together they are found to be non-correlated. This property has

been used to decide on the standard IMF for each person's fingerprint, as discussed in the next section.

3. SVD and Wavelet based Fingerprint Biometric Watermarking

Like our previous work [2] the similar watermarking methodology has been employed here using hybrid format of DWT and SVD [43] [44]. The Watermarking methodology of using hybrid format of the two robust techniques i.e. Discrete Wavelet Transform (DWT) and Singular Value Decomposition (SVD) has been employed here [43] [44]. Cohen-Daubechies-Feauveau (CDF) 9/7 (*'cdf97'*) wavelet have been used here for the lifting-DWT.

3.1. Watermark embedding process

The host image is applied with the single level lifting based DWT to obtain the 4 set of coefficients, i.e., approximate, horizontal, vertical and detailed. They are denoted here as CA, CH, CV, and CD. This is followed up by SVD operation on each of them on similar lines, to get the two orthogonal matrices U and V and the set of Eigen values in S. For the band being CX (CA/CH/CV/CD) the operation is as in equation 2.

$$CX = U \times S \times V^T \tag{2}$$

where CX=CA/CH/CV/CD any of the four coefficients.

The fingerprint template is embedded in the Eigen value matrix S to obtain S^* with CRC_{EMD} which is the EMD based binary code of the fingerprint template in binary, as in equation 3. The CRC used is MATLAB's inbuilt CRC-16 bit [45] [46]. Then SVD is again applied on the S^* matrix to obtain S1, U1 and V1. Here S1 is the Eigen value matrix of S^*, whereas U1 and V1 are the orthogonal matrices.

$$S^* = S + CRC_{EMD} = U1 \times S1 \times V1^T \tag{3}$$

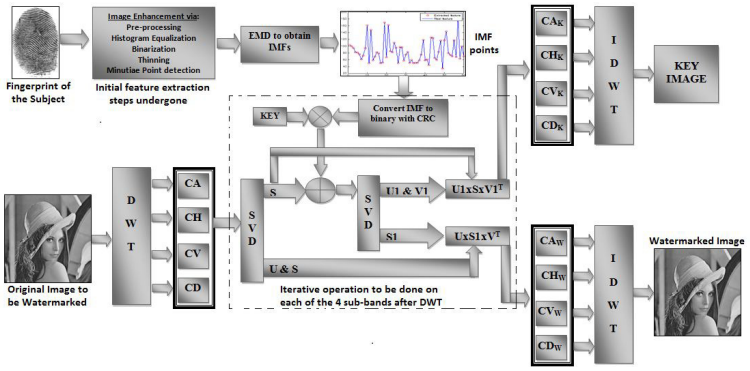


Fig. 2. Fingerprint based Image Watermarking Algorithm

Now the orthogonal matrices of first SVD operation, i.e. U and V, are combined with the Eigen values of the second SVD operation, i.e. S1 to obtain the sub-band for watermarked image i.e. CW. The rest of the Eigen values, U1 and V1 are combined with S, the Eigen values of the first SVD operation to obtain CK, the sub-band for the key image.

$$U \times S1 \times V^T = CW \tag{4}$$

where CW=CA_W/CH_W/CV_W/CD_W any of the four coefficients.

$$U1 \times S \times V1^{T} = CK \tag{5}$$

where $CK=CA_K/CH_K/CV_K/CD_K$ any of the four coefficients.

These operations are applied on all the four sub-bands, to generate the 4 sub-bands for both key image and watermarked image. Then on application of the Inverse Discrete Wavelet Transform (IDWT) on the CA_K, CH_K, CV_K and CD_K generates the Key image. Similarly the watermarked image is generated on application of IDWT on CA_W, CH_W, CV_W and CD_W. The operation is given in Figure 2.

3.2. Watermark extracting process

For the extraction of the watermark from the stego image, the reverse of the above scheme is employed. Here the corrupted version of the watermarked image is considered to be received. Similar to the embedding process, the DWT of the image is taken to obtain the corrupted image's sub-bands CA_C, CH_C, CV_C, and CD_C. The image is decomposed back to its respective coefficients as well. Then the SVD is applied on each respective sub-band pair of corrupted image and key image to obtain U_C, S_C, V_C, U_K, S_K, and V_K respectively. The Eigen values of the stego image, S_C are combined with the respective orthogonal matrices U_K and V_K of the key image to generate the stego sub-band matrix D as in equation 6. The Eigen values of the key image S_K are then subtracted from the matrix D to obtain the watermark coefficients CX_D for that particular sub-band after normalization with the threshold KEY, as in equation 7.

$$D = U_K \times S_K \times V_K^{\,T} \tag{6}$$

$$CX_D = \left(1/KEY\right) \times (D - S_K) \tag{7}$$

where $CX_D=CA_D/CH_D/CV_D/CD_D$ any of the four coefficients.

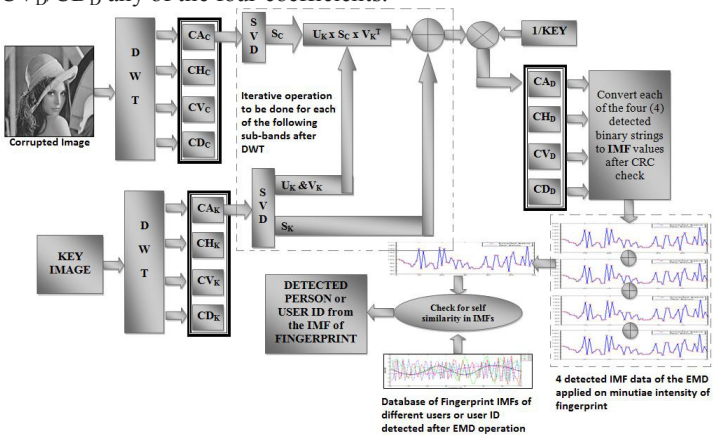


Fig. 3. Watermark Extraction and fingerprint identification Algorithm

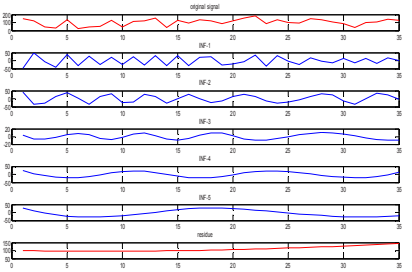


Fig. 4. Partial EMD of any particular fingerprint minutiae intensity to IMFs and residue

So from the watermark coefficients CA_D, CV_D, CH_D, and CD_D obtained the 4 sets of DC values of the iris biometric is retrieved. This is firstly done by removing the CRC error control coding redundant bits first, followed by conversion of the binary data to pixel intensities of the embedded IMF values of the Minutiae. From the set of the four set of IMF values detected from the 4 wavelet sub-bands a normalized set of IMF is obtained. This obtained set of IMF coefficient undergoes self-similarity analysis with the standard sets of IMF stored for each person for detection, authentication and identification of the fingerprint. Based on this fingerprint watermark, the person's identification or detection of the user id of the subscriber is obtained. This is shown in figure 3.

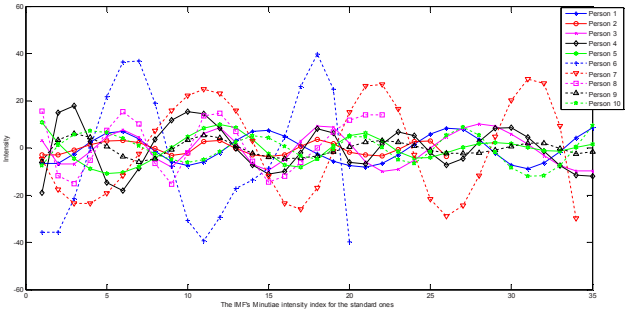
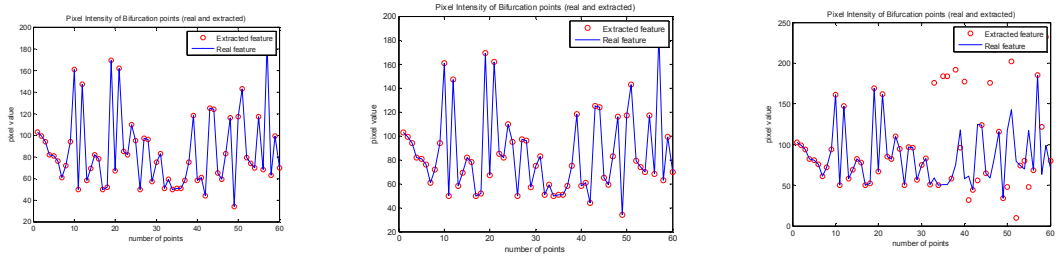
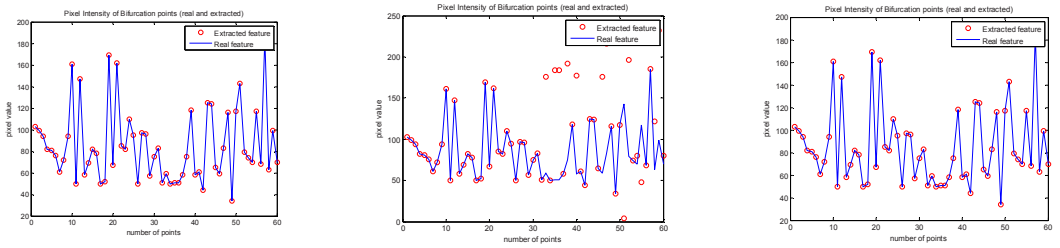


Fig. 5. GEP selected IMF of 10 different persons' after EMD of the Minutiae intensities.



(a) (b) (c)



(d) (e) (f)

Fig. 6. The IMF variation for a particular person for simple attacks like (a) blurring, (b) gaussian filtering, (c) blurring and Gaussian filtering, (d) blurring and median filtering, (e) blurring, median filtering and uniform filtering and (f) all the attacks together except blurring

As the watermark embedded in the image for security is a fingerprint, there must be watermark detection after attacks and the identification of the fingerprint as well. In the FVC 2004 database there are 7 images of the fingerprint of 10 persons. This provides a database of total 70 images for testing the algorithm. The result obtained is nearly at par though the numbers of images are less, the idea of employing EMD based IMFs for fingerprint detection is novel. The operation of EMD on the minutiae intensity for a particular fingerprint can be decomposed to a set of IMFs as shown in the figure 4. Here the intensity is decomposed to 5 IMFs and a residue using EMD are shown for the first 35 points to provide a clear view. For each person, a particular IMF has self similar characteristics with all of his 7 fingerprints. This particular IMF is detected using GEP (Gene Expression Programming) [41] using the GeneXpro software by [42].

4. Result Analysis

The selected standard IMFs are seen to follow a particular type of pattern out here, based on which they can be differentiated. But if the IMFs of different persons' fingerprint for any one image are plotted together they are found to be non-correlated. This can be seen from the non-self similar features of the GEP selected IMFs, in Figure 5 for the 10 users/persons. When the watermarked image, embedded with EMD based fingerprint minutiae feature is attacked by a few popular attacks and their combination the IMF changes for a few cases are shown in Figure 6.

References

[1] S. Majumder, T. S. Das, "Watermarking of data using Biometrics", pg 623-648 Chapter 24, of "Handbook of Research on Computational Intelligence for Engineering, Science and Business", published by IGI Global DOI: 10.4018/978-1-4666-2518-1, ISBN13: 9781466625181, ISBN10: 146662518X, EISBN13: 9781466625198

[2] S. Majumder, K Jilen Kumari Devi, S. K. Sarkar, "Singular value decomposition and wavelet-based iris biometric watermarking", in IET Biometrics, Volume 2, Issue 1, March 2013, p. 21 – 27, DOI: 10.1049/iet-bmt.2012.0052, Print ISSN 2047-4938, Online ISSN 2047-4946

[3] FVC2004: the Third International Fingerprint Verification Competition data base, http://bias.csr.unibo.it/fvc2004/ by the Biometric Systems Lab (University of Bologna), the Pattern Recognition and Image Processing Laboratory (Michigan State University) and the Biometric Test Center (San Jose State University).

[4] S. Majumder, "Iris Biometrics Technologies", pg 20, BIOMETRIC TECHNOLOGIES, dated 11/2012 Hakin9 magazine

[5] R. Kalita, S. Majumder and Md. A. Hussain,"Multidimensional Multimetric Novel and Simple Techniques for Iris Recognition System", International Journal of Recent Trends in Engineering [ISSN 1797-9617], pg 161-166 Volume 3 No 3 May 2010. ACADEMY Publishers, Finland. DOI: 01.IJRTET.3.3.147

[6] S. Majumder, A.D. Singh and M. Mishra,"A GUI based Iris Authentication System for Secured Access" CC2.6 pg 147 to 151 at International Conference on Systemics, Cybernetics, Informatics (ICSCI-2009) under Pentagram Research , Hyderabad held 7-10 January 2009.

[7] S. Majumder, S. Pal, P. K. Dutta, and A. K. Ray, "Wavelet and Empirical Mode Decomposition Based QT Interval Analysis of ECG Signal" pg 247-254 proceedings of 2nd IEEE International Conference on Intelligent Human Computer interaction, (IHCI 2010) ISBN No: 978-81-8489-540-7, organized by IIIT, Allahabad from 16th to 18th January 2010.

[8] N. E. Huang, Z. Shen, S. R. Long, M. C. Wu, H. H. Shih, Q. Zheng, N. C. Yen, C. C. Tung and H. H. Liu , "The empirical mode decomposition and the Hilbert spectrum for nonlinear and non-stationary time series analysis", Proceedings – Royal Society. Mathematical, physical and engineering sciences (1998).

[9] A.Jain, A. Ross, and U. Uludag. Biometric template security: Challenges and solutions. In Proceedings of European Signal Processing Conference (EU- SIPCO), pages 469{472, September 2005.

[10] Anil K. Jain Davide Maltoni. Handbook of Fingerprint recognition. Springer, 2003.

[11] N. N. Rao, P. Thrimurthy, and B. R. Babu, A Novel Scheme for Digital Rights Management of Images Using Biometrics, pg 157-167, International Journal of Computer Science and Network Security, VOL.9 No.3. 2009.

[12] I. T. Lam, and C. M. Pun, Embedding Biometric Watermark on Text Document using Flipping, pg 73-78, Proceedings of the 9th WSEAS International Conference on Multimedia Systems & Signal Processing, ISSN-1790-5117, ISBN: 978-960-474-077-2, 2004

[13] M. K. Dutta, P. Gupta, and V. K. Pathak, Audio Watermarking Using Pseudorandom Sequences Based on Biometric Templates, Journal of computers, vol. 5, no. 3. 2010.

[14] A. E. Hassanien, Hiding Iris Data for Authentication of Digital Images using Wavelet Theory, pg 548-553, proceedings of GVIP 05 Conference, Egypt, 2005.

[15] A. K. Naik, and R. S. Holambe, A Blind DCT Domain Digital Watermarking for Biometric Authentication, pg 11 to 15 of Vol. 1, No. 16, International Journal of Computer Applications, 2010.

[16] M. R. Islam, M. S. Sayeed, and A. Samraj, Biometric Template Protection Using Watermarking with Hidden Password Encryption, pg 296-303, proceedings of International Symposium on Information Technology, Malaysia, 2008.

[17] K. Zebbiche, L. Ghouti, F. Khelifi, and A. Bouridane, Protecting Fingerprint Data using Watermarking, Proceedings of the First NASA/ESA Conference on Adaptive Hardware and Systems (AHS'06), 2006.

[18]D. Mathivadhani, and C. Meena, A Comparative Study on Fingerprint Protection Using Watermarking Techniques, pg 98-102, Global Journal of Computer Science and Technology Vol. 9 Issue 5 (Ver 2.0), 2010.

[19] K. Zebbiche, and F. Khelifi, Region-Based Watermarking of Biometric Images: Case Study in Fingerprint Images, International Journal of Digital Multimedia Broadcasting, Article ID 492942, Pp. 1-13, 2009.

[20] M. Vatsa, R. Singh, A. Noore, M. M. Houck, and K. Morris, Robust biometric image watermarking for fingerprint and face template protection, IEICE Electronics Express, Vol. 3, No.2, Pp. 23-28, 2006.

[21] Y. Li, and S. Du, Biometric Watermarking Based on Affine Parameters Estimation, proceedings of IEEE Conference, 2009.

[22] N. Bartlow,N. Kalka, B. Cukic, and A. Ross, Protecting Iris Images through Asymmetric Digital Watermarking, pg 191-197, proceedings of 5th IEEE Workshop on Automatic Identification Advanced technology (Auto ID), Italy, 2007.

[23] W. Kim, and H. K. Lee, Multimodal biometric image watermarking using two-stage integrity verification, 2385–2399, Elsevier Journal on Signal Processing, 2009.

[24] O. B. Adamo, S. P., Mohanty, E. Kougianos, and M. Varanasi, VLSI Architecture for Encryption and Watermarking Units Towards the Making of a Secure Camera, 2010.

[25] S. P. Mohanty, N. Ranganathan, and R. K. Namballa, VLSI Implementation of Visible Watermarking for a Secure Still Camera Design, Proceedings of International Conference of VLSI Design, pp. 1063–1068, 2004.

[26] J. Daemen, and V. Rijmen, The Design of Rijndael, in Springer- Verlag, 2004.

[27] S. P. Mohanty, K. R. Ramakrishnan, and M. S. Kanakankalli, A DCT Domain Visible Watermarking Techniques for Images, in Proc. of IEEE International Conf on Multimedia and Expo, pp. 1004–1009, 2000.

[28] N. Yager, A. Amin, Fingerprint classification: a review. Pattern Anal Appl 7:77–93, 2004

[29] M. Kawagoe and A. Tojo, Fingerprint pattern classification. Pattern Recognit 17(3):295–303, 1984.

[30] M. Chong, T. Ngee, L. Jun, K. Gay, Geometric framework for fingerprint image classification. Pattern Recognit 30(7– 9):1475–1488, 1997.

[31] R. Cappelli, A. Lumini, D. Maio, D. Maltoni, Fingerprint classification by directional image partitioning. IEEE Trans Pattern Anal Mach Intell 21(5):402–421, 1999.

[32] R. Cappelli, D. Maio, D. Maltoni, A multi-classifier approach to fingerprint classification. Pattern Anal Appl 5:136–144, 2002

[33] A. Jain,S. Prabhakar, L. Hong, A multichannel approach to fingerprint classification. IEEE Trans Pattern Anal Mach Intell 21(4):348–359, 1999.

[34] D. Ruta, B. Gabrys, An overview of classifier fusion methods. Comput Inform Syst 7(1):1–10, 2000.

[35] A. Ross, J. Shah, A. Jain, Towards reconstructing fingerprints from minutiae points. In: Proceedings of SPIE conference on biometric technology for human identification II, 2005.

[36] X. Tan, B. Bhanu,Y. Lin, Fingerprint classification based on learned features. IEEE Trans Syst Man Cybern Part C: Appl Rev 35(3):287–300, 2005

[37] FVC2004: the Third International Fingerprint Verification Competition data base, http://bias.csr.unibo.it/fvc2004/ by the Biometric Systems Lab (University of Bologna), the Pattern Recognition and Image Processing Laboratory (Michigan State University) and the Biometric Test Center (San Jose State University).

[38] Jyh-Chian Chang; Ming-Yu Huang; Jen-Chun Lee; Chien-Ping Chang; Te-Ming Tu, Iris recognition with an improved empirical mode decomposition method, SPIE Proceedings Vol. 48 Optical Engineering 48(04), 047007

[39] J.R. Koza, Genetic Programming: On the Programming of Computers by Means of Natural Selection, MIT Press (1992),

[40] C. Ferreira, Gene Expression Programming: Mathe-matical Modeling by an Artificial Intelligence (2nd Edition) [M]. Springer Verlag Berlin Heidelberg, 2006.

[41] C. Ferreira, "Gene Expression Programming: A New Adaptive Algorithm for Solving Problems". Complex Systems, Vol. 13, issue 2: 87–129, 2001.

[42] GepXpro 4 from http://www.gepsoft.com

[43] S. Majumder, T. S. Das, V. H. Mankar, S. K. Sarkar, "SVD and Error Control Coding based Digital Image Watermarking", pg 60-63, proceedings of International Conference on Advances in Computing, Control and Telecommunication Technologies'2009(ACT 2009), published by IEEE Computer Society, ISBN 978-0-7695-3915-7 , 2009.

[44] M. Saikia, S. Majumder, T. S. Das, Md. A. Hussain, S. K. Sarkar, "Coded Fingerprinting Based Watermarking to Resist Collusion Attacks and Trace Colluders", pg 120-124, proceedings of International Conference in Advances in Computer Engineering(ACE-2010) ISBN - 978-1-4244-7154-6 DOI 110.1109/ACE.2010.36 published by IEEE CS DL on 2010.

[45] Bernard Sklar, Digital Communications: Fundamentals and Applications. Englewood Cliffs, N.J., Prentice-Hall, 1988.

[46] Stephen B. Wicker, Error Control Systems for Digital Communication and Storage, Upper Saddle River, N.J., Prentice Hall, 1995.