Global Journal of Computer Science and Technology: F
Graphics & Vision
Volume 15 Issue 4 Version 1.0 Year 2015
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

Intensifying the Security of Multiomodal Biometric Authentication System using Watermarking

By Shashi Choudhary & Naveen Choudhary

College of Technology & Engineering Udaipur, India

Abstract- In Multimodal biometrics system two or more biometric attributes are combined which makes it far more secure than unimodal system as it nullifies all the vulnerabilities of it. But with the prompt ontogenesis of information technology, even the biometric data is not secure. There is one such technique that is implemented to secure the biometric data from inadvertent or deliberate attacks is known as Digital watermarking. This paper postulate an approach that is devise in both the directions of enlarging the security through watermarking technique and improving the efficiency of biometric identification system by going multimodal. Three biometric traits are consider in this paper two of them are physical traits i.e. ; face, fingerprint and one is behavioral trait (signature).The biometric traits are initially metamorphose using Discrete Wavelet and Discrete Cosine Transformation and then watermarked using Singular Value Decomposition. Scheme depiction and presented results rationalize the effectiveness of the scheme.

Keywords: discrete cosine transform (dct), discrete wavelet transform (dwt), singular value decomposition, multimodal biometrics, watermarking.

GJCST-F Classification: D.4.6

Intensifying the Security of Multiomodal Biometric Authentication System using Watermarking

Shashi Choudhary [α] & Naveen Choudhary [σ]

Abstract- In Multimodal biometrics system two or more biometric attributes are combined which makes it far more secure than unimodal system as it nullifies all the vulnerabilities of it. But with the prompt ontogenesis of information technology, even the biometric data is not secure. There is one such technique that is implemented to secure the biometric data from inadvertent or deliberate attacks is known as Digital watermarking. This paper postulate an approach that is devise in both the directions of enlarging the security through watermarking technique and improving the efficiency of biometric identification system by going multimodal. Three biometric traits are consider in this paper two of them are physical traits i.e. ; face, fingerprint and one is behavioral trait (signature).The biometric traits are initially metamorphose using Discrete Wavelet and Discrete Cosine Transformation and then watermarked using Singular Value Decomposition. Scheme depiction and presented results rationalize the effectiveness of the scheme.

Keywords: discrete cosine transform (dct), discrete wavelet transform (dwt), singular value decomposition, multimodal biometrics, watermarking.

I. Introduction

In this span of Electronic advancement and Information technology, electronic access/verification of individuals to service or work place is becoming crucial so as to prevent any act of compromise to the integrity of the organization or individual. Authenticating the identity of an individual is imperative for completion of all personal or commercial transactions. We can obviate forgery and fraudulent activities if one initiates its identity with conviction which is unattainable in case of traditional authentication system that are either knowledge based or token based. This has shepherd in the emergence and genesis of a new technological area known as biometric recognition, or merely expressed as biometrics [1]. Biometric is a unique feature, a measurable trait or characteristic which is utilized in electronically identifying or verifying the identity of a human being. Biometrics which is an ominous combination of modern science and technology with human attributes can be used to protect and secure our material information/data and property. Biometrics system is referred to as the automated means of identification of individuals based on their physiological characteristics like fingerprints, iris, hand geometry, face recognition etc. or behavioral characteristic that include voice, gait recognition, keystroke scanning, signature-scan. Biometric attributes of the user are abiding and also these characteristics are unique for every individual and cannot be altered or lost easily. Thus biometrics is believed to be an authentic technology and more advanced in comparison to other contemporary techniques. Biometric authentication systems have inherent advantages over conventional personal identification techniques [2]. However, the security of biometrics data is preeminent and must be shielded from external intrusion and tampering as they are not endowed with security themselves [1]. It is therefore of utmost importance to provide security to the biometric templates of individuals at all times.

Encryption is a way to address this issue [3, 4]. Encryption does not subscribe to the much needed mutually integrated security and is futile once the data is decrypted after it is being transmitted over the network. Cryptography uses methods of encryption to generate secure information. As encryption and cryptography are not fully competent of creating security throughout the life of the work [4], digital watermarking has emerged as a plausible solution. A segment of information termed as watermark, is embedded into the cover image using a secret key, in such a way that the data of the cover image are not amend to the extent that are perceptible to the Human Visual System is termed as biometric watermarking. There are two type of biometric system one is unimodal and other is multimodal biometric system. The unimodal biometric modalities may not fulfill the demand of challenging applications in terms of acceptability, collectability, circumvention, universality, uniqueness, performance, permanence. These factors paved a way for the development of multimodal biometric authentication system. More than one biometric character is used in order to identify an individual in multimodal biometric system. Multimodal biometric systems provide higher recognition rate in compare to unimodal systems [5]. The physical biometric modalities, such as fingerprint, face and iris are widely used conventional and effective modalities [6].

Author α σ: Department of Computer Science, and Engineering, College of Technology & Engineering Udaipur, India.
e-mail: shashichoudhary1991@gmail.com

This paper emphasizes on watermarking face image, fingerprint image and with signature image by using a robust watermarking scheme, for intensifying the security and performance of multimodal biometrics authentication system. It also emphasizes on comparing both the images with the original images in order to verify that it does not affect the recognition capacity of the overall system by watermarking and extraction procedure.

II. Background Details

a) Watermarking

To authenticate image and prevent it from forgery watermarking is being used for centuries. Watermarking [7,8,9] is the technique of embedding data into elements such as an image, audio or video file for authentication purpose. Presently, watermarks are embedded in digital images so that authorized person can propound ownership and confirm the validity of their data values. There are numerous applications where security is a vital issue so in those cases embedded watermark must be invisible, robust and should have a high capacity .Generally watermarking is used for hiding information imperceptibly in digital text for shielding its integrity. The necessity for watermarks in varied scenarios differ as per their need. Embedding a single watermark into the content at the source of distribution is sufficient for identification of the origin of content [11]. Unique watermark is required for tracing illicit copies, based on the identity or location of the recipient in the network.

Recently, a number of watermarking schemes have been developed using two of the most popular transforming techniques which are Discrete Cosine Transform (DCT), and Discrete Wavelet Transform (DWT). The generic model of watermark embedding and extraction is shown in Fig. 1.

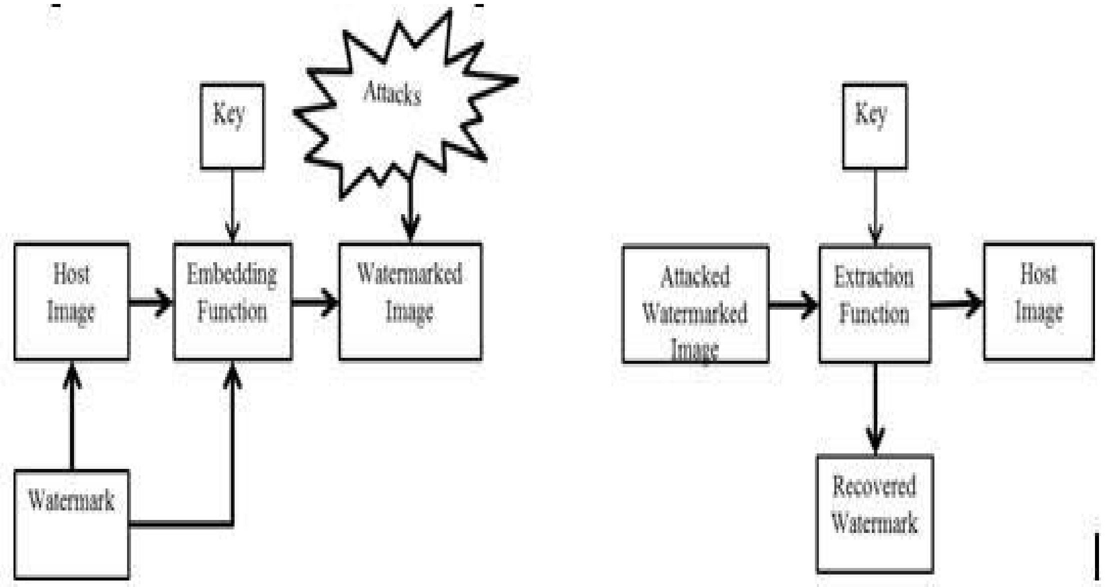


Fig.1: Model for Watermark embedding and extraction

Initially, in embedding module first of all the host image is watermarked with the data/message image using a embedding function and secret key. Then the watermarked image is stow in Database or relay through the network where there is a feasibility that it may be attacked or confronted. While in extraction procedure the extraction part the watermarked image which might have been confronted is enhance to the extraction function beside with the secret key and the watermarked image is extracted from it.

b) Discrete Wavelet Transform

Wavelet Transform uses a wavelet of finite energy. The *discrete wavelet transform* (DWT) is an contraption of the *wavelet transform* using a *different* set of the *wavelet* scales and translations heed some *defined* rules. The key abstraction of Discrete Wavelet Transform is that a 1-D signal is cleave into two parts i.e.; one is low frequency band and another is high frequency band. Then the low frequency band is farther split into two parts and the same process pursue until the desired level is reached.

For M*N 2-D images, applying DWT corresponds to processing the image by 2-D filters in each dimension and results in the generation of four M/2*N/2 coefficients. The filters split the input image into four non-overlapping multi-resolution coefficient sets (LL1), (HL1), (LH1) and(HH1). Where (LL1) is a lower resolution approximation image,(LH1) vertical high frequency band,(HL1) horizontal high frequency band, and (HH1) diagonal high frequency band. Low frequency band having the information of an image near to the original image. In DWT decomposition, input signal must be a multiple of 2^n[15]. Where, n is equivalent to the number of levels. Moreover, DWT provides ample information to scrutinize and unify the actual signal and also requires less computation time. Fig. 2 present the two-level DWT decomposition of an image.

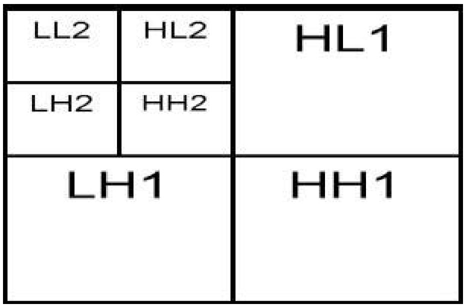


Fig. 2 : Two level DWT decomposition

c) *Discrete Cosine Transform*

DCT is one of the most prevalent transform domains watermarking techniques.DCT transform spatial or time domain signal to frequency domain and the image is amend into a form of an even functions[15]. DCT is more robust in comparison to spatial domain. Algorithms based on DCT are vigorous against recurrent image processing operations like adjustment, brightness, blurring, contrast, low pass filtering, and so on. One-dimensional signals like speech waveforms can be sort out with one dimensional DCT. For scrutiny/perusal of 2D signals like images, we need 2-D DCT.

The 2D DCT of any given matrix gives the frequency coefficients in context of another matrix. The highest frequency coefficients are depicted at the Right bottom most corner of the matrix while the lowest frequency coefficients are depicted at the left top most corner of the matrix.

Formula for 2-D DCT:

$$F(m,n) = \sum_{i=0}^{N-1} \sum_{j=0}^{N-1} C(m)\,C(n)\,f(i,j) \cos\left[\frac{\pi(2i+1)m}{2N}\right] * \cos\left[\frac{\pi(2j+1)m}{2N}\right]$$

Formula for 2-D inverse DCT:

$$F(i,j) = \sum_{i=0}^{N-1} \sum_{j=0}^{N-1} C(m)\,C(n)\,F(m,n) \cos\left[\frac{\pi(2i+1)m}{2N}\right] * \cos\left[\frac{\pi(2j+1)m}{2N}\right]$$

Where,

$$C(m), C(n) = \begin{cases} \sqrt{\frac{1}{N}} & |m,n = 0 \\ \sqrt{\frac{2}{N}} & |m,n = 1\ upto\ N-1 \end{cases}$$

d) *Singular Value Decomposition*

SVD is powerful mechanism for image transformation. SVD is based on a theorem from linear algebra which states that a rectangular matrix A can be cleave into the product of three matrices; U - an orthogonal matrix, S- a diagonal matrix, and V - the transpose of an orthogonal matrix.

The theorem is represented as:

$$A_{m*n} = U_{m*m}\ S_{m*n}V^T_{n*n}$$

Where;

$$U^TU = I;\ V^TV = I;$$

The columns of U are orthonormal eigenvectors of AA^T, The columns of V are orthonormal eigenvectors of A^TA, and S represent the diagonal matrix that hold the square roots of eigen values from U or V in descending order.

III. The Proposed Method

One biometric data is watermarked with another biometric data using SVD based hybrid watermarking scheme. In the propound scheme face image is used as the host image or cover image which is watermarked using the fingerprint and signature image. The Hybrid watermarking technique is delineate algorithmically as well as schematically.

a) Watermark Embedding Algorithm

First of all we take face image as a cover image, weinput the Cover image I and exert DWT on the Cover image I, DWT crumble image into four sub-bands LL, HL, LH and HH Moreover after decomposing into four sub-bands DCT is applied to all the high frequency bands and SVD is also applied to all the high frequency bands to attain the matrices SH1_I, SH2_I and SH3_I. Both Watermark images W1,W2 is given as input then DWT is applied on the Watermark images W1,W2 which crumble into two pair of four sub-bands LL1, HL1, LH1, HH1, LL2, HL2, LH2, HH2. DCT is applied to all high frequency bands further SVD is applied to all the higher frequency bands and acquire the relevant matrices .Deploy the singular values of Watermark images the singular values of the cover image are modified. Modified SVD matrix is constructed by this. Inverse DCT is applied to all high frequency bands then inverse DWT is utilize to obtain the final watermarked image.

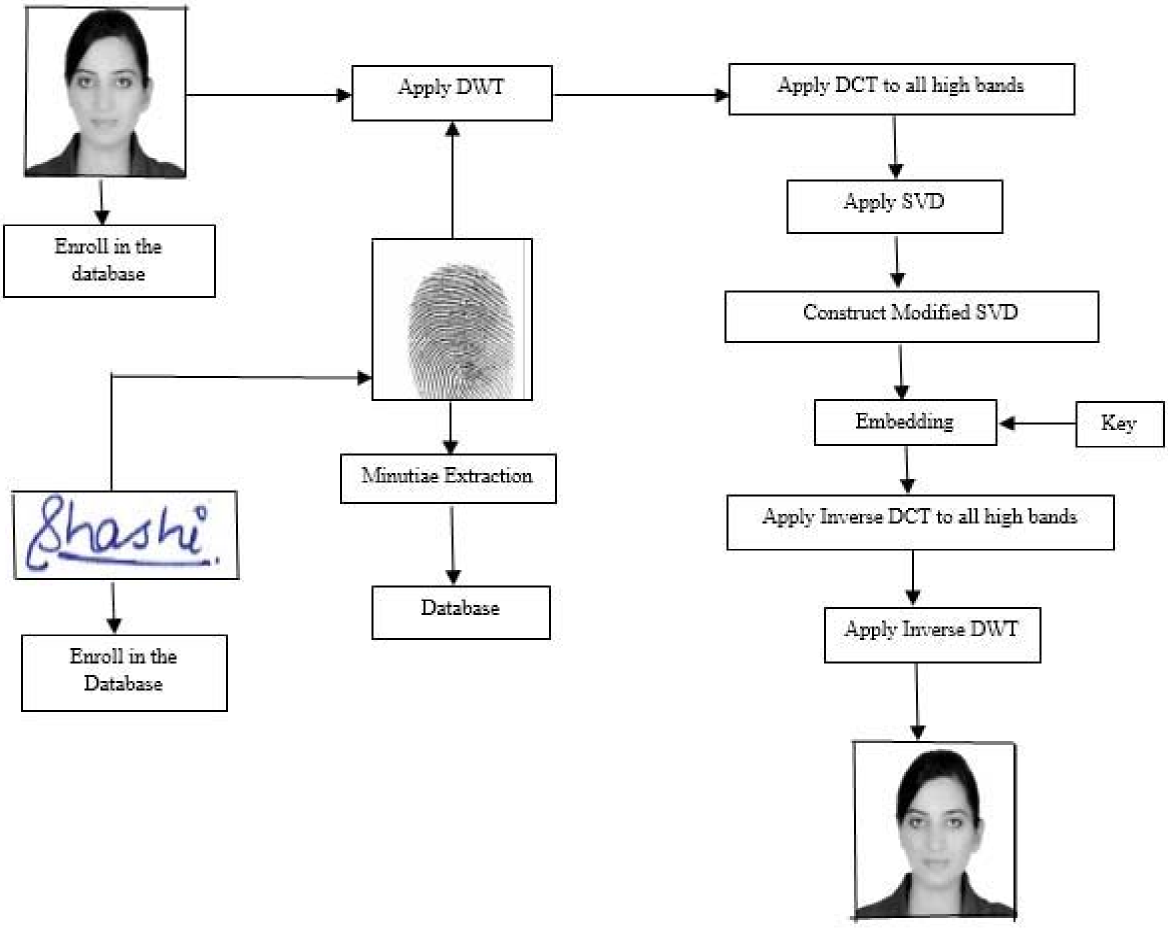


Fig.3 : Watermarking Embedding Machanism

b) Watermark Extraction Algorithm

Input Watermarked image is taken as W_I. DWT is utilize on the Watermarked image W_I; it decomposes image into four sub-bands LL_W, HL_W, LH_W and HH_W. All high frequency bands are stipulated and DCT is applied to all high bands. Then SVD is applied to all the high frequency bands to obtain the matrices SH1_WI, SH2_WI and SH3_WI.SH1_WI, SH2_WI and SH3_WI are altered. Modified SVD matrix is constructed. To all high frequency bands Inverse DCT is applied. Inverse DWT is applied to obtain the final extracted watermark image.

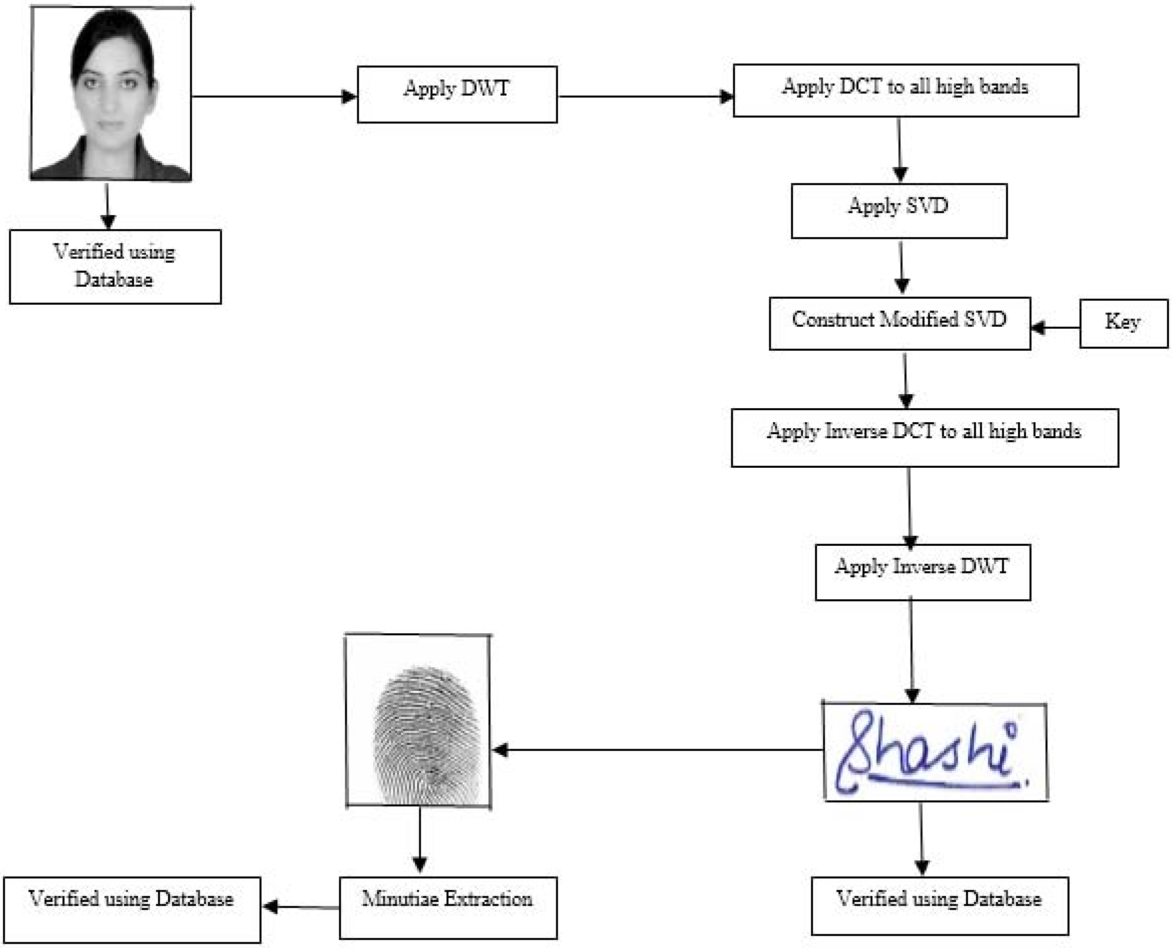


Fig.4: Watermarking Extraction Mechanism

IV. Implementation and Results

"Watermarking is the process that embeds data called a watermark or tag into any object such that watermark can be detected or extracted later to make an assertion about the data". Watermarking algorithm can be evaluated by Its Performance, Robustness and imperceptibility. Imperceptibility means the perceived quality of cover image should not be distorted by presence of watermark.

Peak Signal to Noise Ratio is used in perceptible analyzing the concealing capacity of the algorithm. Peak Signal to Noise Ratio (PSNR) is calculated between original and watermark image. The larger the value of PSNR is, the better the imperceptibility of watermark. Peak Signal to Noise Ratio (PSNR) is determine by:

$$\text{PSNR} = 10\log_{10}\left(\frac{255^2}{MSE}\right)$$

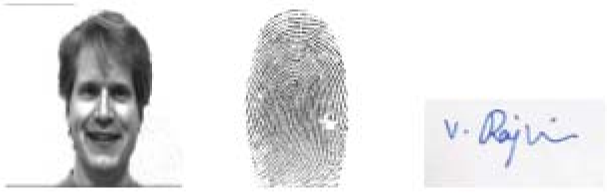
The unit is decibels (dB).The correlation or similarity between the original watermark and the extracted watermark is computed by utilizing Normalized Cross-Correlation [12].

The formula for Normalized Cross-Correlation (NCC) is

$$\text{NCC} = \sum_i \sum_j \frac{w(i,j)w'(i,j)}{\sum_i \sum_j |w(i,j)|^2}$$

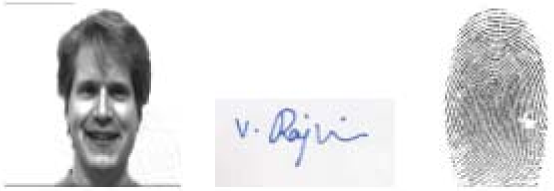
The value of Normalized Cross-Correlation lies between [-1, 1]. If the Extracted watermark absolutely tally with the original image, the Normalized Cross-Correlation (NCC) =0.9987. Otherwise NCC is between 0 and 1.

Simulation is done on MATLAB2013b and by simulating the experiment performance of the algorithm is tested. 256x256 pixels of gray-level cover image and watermark image are chosen for the purpose of simulation of the algorithm. The original cover image, watermarked images and the extracted watermark images are shown in Fig.5.



Original cover image Original Watermak1 Original Watermark2

Fig.5: [A] Original Cover Image and Watermark image



Watermarked image Extracted watermak1 Extracted watermark2

Fig.5: [B] Watermark image and Extracted Watermarks

The watermarked image look like the original image in vision impression to a large expanse. Generally there is no clearly visible difference between the images for the Human Visual System. Therefore, this algorithm is quite good in hiding watermark. By this algorithm weobtain PSNR value between the original cover image and watermarked image which is 52.51 dB, which is reckoned as a quite good value. Along with that, the Normalized Cross-Correlation (NCC) of the original watermark image and extracted watermark is 0.9998, which shows that the two images are strongly correlated. Fig.6 shows the comparison of PSNR.

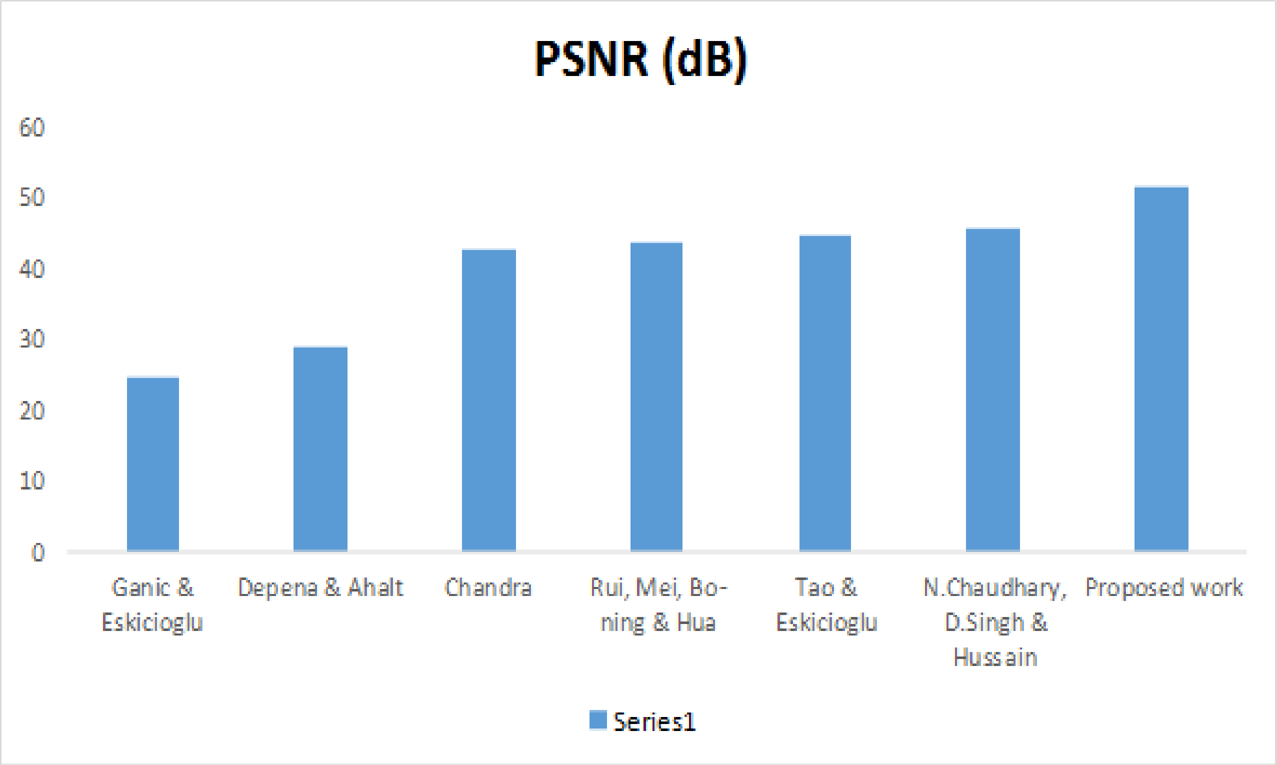


Fig. 6 : Graph showing the comparison of PSNR

V. Conclusion

In this paper, a robust watermarking algorithm is proposed. Two watermarks images, a fingerprint and a signature is watermarked over a cover image i.e.; face image. This paper propound a discrete wavelet transform and discrete cosine transform based watermarking algorithm for biometric data. Watermarking signals are embedded in the high frequency parts of wavelet transformation domain by using Singular Value Decomposition. And before the embedding, procedure is stalked by the watermark image is also transformed using both DWT and DCT. Quantitative results show that the fingerprint, face and signature images are of good quality, after extraction of watermark the quality of host image remains quite good, also it robust against many image processing operations. This algorithm is very efficient in embedding signals.

References Références Referencias

1. K. Jain, U. Uludag, Hiding Biometric Data, *IEEE Trans. Pattern Analysis and Machine Intelligence, 25(11),* Nov. 2003, 1494 – 1498.
2. K. Jain, A. Ross, and S. Prabhakar, An introduction to biometric recognition, *IEEE Transactions on Circuits and Systems for Video Technology, 14 (1),* 200,4-20.
3. U. Uludag, S. Pankanti, S. Prabhakar, and A.K. Jain, Biometric cryptosystems: issues and challenges, *Proceedings of IEEE, 92(6),*2004, 948-960.
4. Y. Dodis, L. Reyzin, and A. Smith, Fuzzy extractors: how to generate strong keys from biometrics and other noisy data,*Eurocrypt*2004, 523-540.
5. A.Nagar, K.Nandakumar, A. K.Jain, Multibiometric Cryptosystems Based on Feature-Level Fusion, *IEEETrans. Inf. Forensics Security, 7(1),* Feb. 2012, 255–268.
6. Z. huiming, Z.Huile, A technology of hiding fingerprint minutiae in image, *Research& progress of solid state electronics, 26(2),*2006, 197-200.
7. I. Podilchuk and E. J. Delp, Digital Watermarking: Algorithms and Applications, IEEE *Signal Processing Magazine,* July 2001, 33-46.
8. I. J. Cox, M. L. Miller, and J. A. Bloom, *Digital Watermarking* (Morgan Kaufmann Publishers, 2002).
9. E. T. Lin, A. M. Eskicioglu, R. L. Lagendijk and E. J. Delp, Advances in Digital Video Content Protection, *Proceedings of the IEEE, Special Issue on Advances in Video Coding and Delivery, 2004.*
10. G.C. Langelaar, I. Setyawan, R.I. Lagendijik, Watermarking digital image and video data, *IEEE Signal Processing Magazine 17 (5)2000, 20–46.*
11. N.F. Johnson, Z. Duric and S. Jajodia, *Information Hiding, Steganography and Watermarking-Attacks and Counter Measures*, Kluwer academic publisher, 2003, 15-29.
12. M. Nageshkumar , P.K. Mahesh , M. N. Shanmukha Swamy, An Efficient Secure Multimodal Biometric Fusion Using Palmprint and Face Image, *IJCSI International Journal of Computer Science Issues*, 2, Aug. 2009,49-53.
13. J Jiang, A. Armstrong, Data hiding approach for efficient image indexing, *Electronics letters. 7th, 38(23),* 2002, 1424- 1425.
14. I.J .Cox, J.G. Linnartz, Some general methods for tampering with watermarks, *IEEE Journal on Selected Areas inCommunications,16(4),*1998, 587-593.
15. Dr. N. Chaudhary, Dr. D. Singh, D. hussain, Enhancing Security of Multimodal Biometric authentication System by Implementing Watermarking Utlizing DWT and DCT, *IOSR Journal of Computer Engineering (IOSR-JCE,), p- ISSN: 2278-8727Volume 15, Issue 1 (Sep. - Oct. 2013.*
16. Pradeep Kumar, Shekhar Singh, Ashwani Garg and Nishant Prabhat , Hand Written Signature Recognition and Verification using Neural Network, *International Journal Of Advance research in Computer Science and Software Engineering*, Volume 3, Issue 3, March 2013.
17. U. Dieckmann, P. Plankensteiner, and T. Wagner. Sesam: A Biometric Person Identification using sensor Fusion. Pattern Recognition Letters, 18(9):827-833, 1997.

This page is intentionally left blank