ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 2.114

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

FINGERPRINT BASED IMAGE STEGANOGRAPHY IN TRANSFORM DOMAIN

Hetal R. Patel, Khushboo Sawant, Krishnakant Kishore
Research scholar, Assistant Professor , Assistant Professor & Head
Computer Science Engineering, JDCT, Indore, India

ABSTRACT

A motivation for the use of Steganography techniques in biometric systems has been the need to provide increased security to the biometrics data themselves. Fingerprints are unique biometrics mainly used for the establishment of direct personal identity but they are at risk to accidental attacks. Protection of biometric data is one of the most important concerns these days and therefore it is gaining interest among researchers. Many security concerns are raised through the storing and transferring of biometric data, which is sensitive and may be impossible to recover if lost, counterfeited, or hacked.There are two possible domain for fingerprint based stgenography,Spatial domain and Transform domain.Transform based steganography provide more capacity, robustness and security. In transform Domain use discrete wavelet transform,it provide more robustness and capacity. In this Review paper describe about the Fingerprint based Steganography in transform domain.

KEYWORDS: Fingerprint Image, Steganography, Discerte Wavelet Transform,Watermark,Haar

INTRODUCTION

Steganography is a type of hidden communication that literally means "covered writing" (from the Greek words stegano or “covered” and graphos or “to write”). The goal of steganography is to hide an information message inside harmless cover medium in such a way that it is not possible even to detect that there is a secret message. A fingerprint is represented by the impression of the pattern of ridges and valleys on the surface of a fingertip. The uniqueness of a fingerprint is determined by the combination of the pattern of ridges and valleys and the minutiae points [5]. Due to their uniqueness, fingerprint images are usually used for user authentication purposes. Consequently, their protection has become an extremely important issue.

A digital watermark algorithm is one of the most researched methods to protect fingerprint images and there are several characteristics that a good watermark technique should include. For example, it should be perceptually invisible and resistant to common image processing operations. There are two main challenges for fingerprint watermarking algorithms which are designed to protect fingerprint images.Watermarking of fingerprint images can be used to secure central databases from which fingerprint images are transmitted on request to intelligence agencies in order to use them for identification purposes. Here, if due to some incidental/intentional tampering, the received fingerprint is falsely matched to someone else, the extracted watermark plays the role of a scrutinizer that can be used to check whether the fingerprint received is of the same person whose label it holds or not [1]. Biometrics based authentication systems are becoming increasingly popular as they offer enhanced security and user convenience as compared to traditional token-based (I.D. card) and knowledge based (password) systems. With the increasing usage of biometric systems the problem of storing the sensor data has become an important issue. Also in most of the cases the sensor data has to be transferred via a communication channel with low bandwidth and high latency. Therefore minimization of the amount of data is highly desirable which is achieved by compressing [2] the data before transmission.

An information-hiding system is characterized by having three different aspects that contend with each other. These are, capacity, security, and robustness as shown in Fig.1. Capacity refers to the amount of information that can be hidden in the cover medium, security to an eavesdropper’s inability to detect hidden information, and robustness to the amount of modification the stego medium can withstand before an adversary can destroy hidden information.

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 2.114

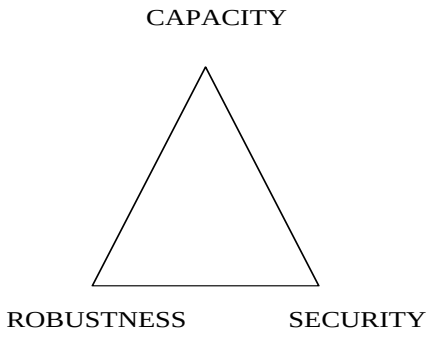

Fig 1. Information-hiding system features [14]

Generally speaking, information hiding relates to both watermarking and steganography. A watermarking system primary goal is to achieve a high level of robustness—that is, it should be impossible to remove a watermark without degrading the data object's quality. Steganography, on the other hand, strives for high security and capacity, which often entails that the hidden information is fragile. Even trivial modifications to the stego medium can destroy it [14].

DOMAIN OF FINGERPRINT STEGNOGRAPHY

Image steganography techniques can be classified into two broad categories: Spatial-domain based steganography and Transform domain based Steganography in fig 2.

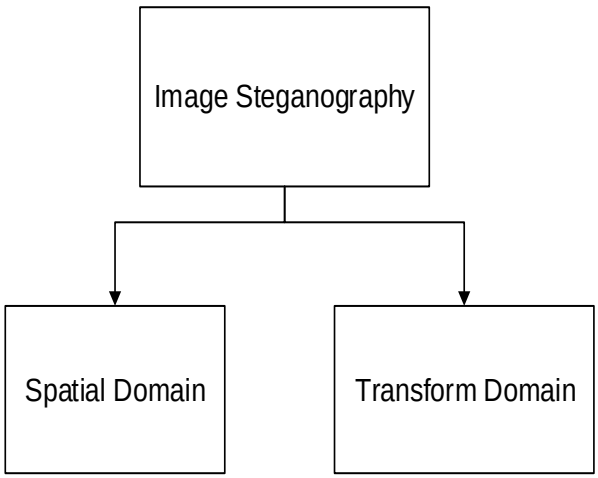

Fig 2. Domain of Fingerprint Steganography

SPATIAL (TIME) DOMAIN BASED STEGANOGRAPHY

In spatial domain scheme, the secret messages are embedded directly. Here, the most common and simplest steganography method is the least significant bits (LSB) insertion method. In the LSB technique, the least significant bits of the pixels are replaced by the message bits which are permuted before embedding.Most steganography software hide information by replacing only the least significant bits (LSB) of an image with bits from the file that is to be hidden. This technique is generally called LSB encoding. An example of this technique is the least significant bit (LSB) method where watermark data is embedded into the least significant bit. The technique has several advantages such as a low level of complexity and ease of implementation. In contrast, LSB is not recommended for watermarking algorithms due to the fact that they are not robust to some image attacks, in particular to lossy compression [5].

TRANSFORM DOMAIN BASED STEGANOGRAPHY

The transform domain steganography technique is used for hiding a large amount of data with high security, a good invisibility and no loss of secret message. The idea is to hide information in frequency domain by altering magnitude of all coefficients of cover image. It converts image blocks from spatial domain to frequency domain.

Transform domain steganography methods can be classified into as follows.

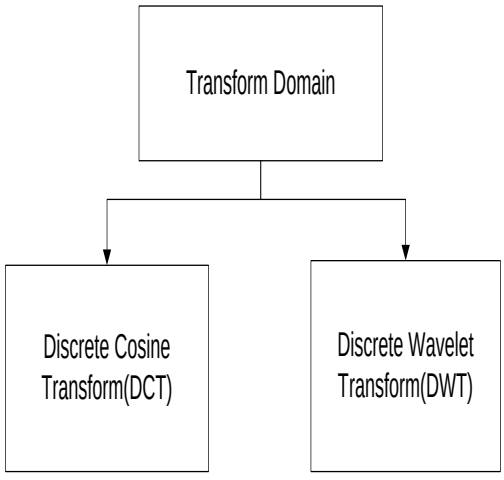

Fig 3. Method of Fingerprint Steganography

On the other hand, transform domain methods are widely used for robust watermarking algorithms where the watermark is embedded by modifying the frequency coefficient [5]. Popular examples of these techniques are the Discrete Cosine Transform (DCT) and the Discrete Wavelet Transform (DWT). While

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 2.114

DCT [2] and DWT [1] are widely used for watermarking methods.Determining the frequency band to embed the watermark pattern in the transform domain algorithms is an important issue. In general, the most significant bit is not preferred part in which to embed a robust watermark because it may affect the watermark perceptually where the watermark may become visible [5]. Thus, specifying where to embed the watermark is a tradeoff between perception and robustness.

HAAR DISCRETE WAVELET TRANSFORM

HDWT is the easiest and most commonly used method. HDWT can be implemented by two procedures: (1) Horizontal Operation and (2) Vertical Operation. First the Horizontal Operation is utilized to decompose an image into a low frequency band (L) and a high frequency band (H). Second Vertical Operation is utilized to partition L and H into LL, LH, HL and HH different frequency bands, each of which possesses ¼ of the original image size. HH represent High Frequency band, LL is low frequency band and LH & HL are middle frequency bands. The coefficients in LL are paramount. If any of the coefficients in LL frequency band are changed, observer can visibly see that the corresponding spatial domain image has been changed. Human eyes are not sensitive to change of HDWT coefficients in HH. For any reason, when any coefficients in HH are altered, an observer can arduously (difficultly) distinguish the change in the spatial domain image.

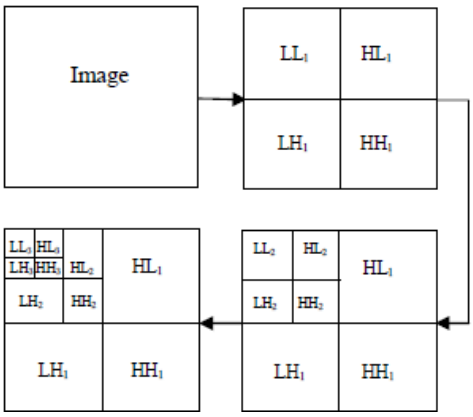

Fig 4. 3-level of 2-D DWT

Fig 5. Original Fingerprint Image

Fig 6. 1-level Of 2-D DWT

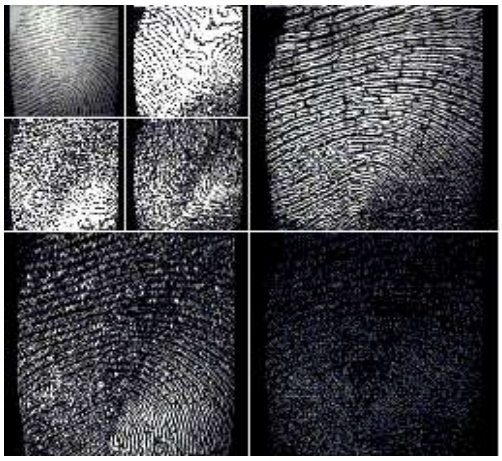

Fig 7. 2-level Of 2-D DWT

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 2.114

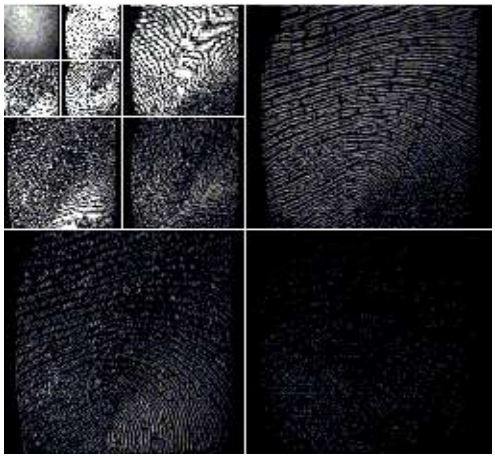

Fig 8. 3-level Of 2-D DWT

Fingerprint Image show in fig 5, apply 2-D Dwt on it generate 1-level 2-D DWT show in Fig 6.Now apply 2-D DWT on Fig 6 genetrate 2-level 2-D DWT show in Fig 7.and last apply 2-D Dwt on Fig 7 generate 3-level 2-D DWT show in fig 8.

LITERATURE REVIEW

This section describes the previous work which had been done for FingerPrint Based Steganography in Transform Domain.

Rajlaxmi Chouhan et al., [1] proposed Fingerprint Authentication by Wavelet-based Digital Watermarking. The DWT based technique has been found to give better robustness against noises, geometrical distortions, filtering and JPEG compression attack than other frequency domain watermarking techniques.

Ameya K. Naik et al., [2] presented an efficient blind digital image watermarking algorithm using mapping technique. The algorithm can embed or hide an entire image or pattern (logo) directly into the original image. The embedding process is based on changing the selected DCT coefficients of the host image to odd or even values depending on the binary bit value of watermark DCT coefficients.

Cameron Whitelam et al., [3] presented an approach for hiding biometric data, which utilizes a combination of asymmetric digital watermarking and steganography. The combination of these techniques enables the system to handle many issues associated with storing and transferring raw biometric data.

Mohammed Alkhathami et al., [4] proposed an approach for embedding two watermarks into fingerprint images using the Discrete Cosine Transform (DCT) algorithm. The main aim of the proposed algorithm is to add more authentication factors based on the watermark messages and to protect the ownership of the fingerprint image. Since the information used for identification or verification of a fingerprint image mainly lies in its minutiae, the introduced watermarking algorithm does not affect fingerprint features.

Mohammed Alkhathami et al., [5] proposed a new digital watermarking technique for fingerprint images using the Dual-Tree Complex Wavelet Transform (DTCWT). The watermark is embedded into the real and imaginary parts of the DTCWT wavelet coefficients. This work focuses on the study of watermarking techniques for fingerprint images that are collected from different angles without corrupting minutiae points.

Khalil Zebbiche et al., [6] introduce a multiresolution wavelet-based digital watermarking method to hide biometric data (i.e. fingerprint minutiae data) into fingerprint images. This method doesn't require the original image to extract the embedded minutiae.

Anil K. Jain et al., [7] presented a fingerprint image watermarking method that can embed facial information into host fingerprint images. This scheme has the advantage that in addition to fingerprint matching.

Yung kuan chan et al., [8] developed proposed method that transform a spatial domain cover image into a frequency domain image using Haar digital wavelet transform method, compresses coefficients of the high frequency band by the Huffman or arithmetic coding method and then embeds the compression data and secret data in high frequency band. This method utilizes the Huffman coding to recover the cover image without any distortion.

Vikas pratap and Prof. Shrikant [9] proposed a new frequency domain method using Haar Wavelet for image steganography. The merit is to increase image quality by hiding the messages in HL, LH, and HH sub-bands while keeping LL sub-band invariant. The advantage of this is that the original cover image does not have to be present on the receiver side.

Mayank Vasta et al., [10] presented a novel biometric watermarking algorithm for improving the recognition accuracy and protecting the face and fingerprint images from tampering. Multi-resolution Discrete Wavelet Transform is used for embedding the face image in finger print image. An intelligent learning algorithm based on SVM (Support Vector Machine) is introduced to enhance the quality of extracted face image.

Mayank Vasta et al., [11] presented a combined DWT and LSB based biometric watermarking algorithm that securely embeds a face template in a fingerprint image. The proposed algorithm is robust to geometric and frequency attacks.

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 2.114

V.Chandra Prasad et al., [12] a block cipher called AES-128 bit key encryption algorithm and DCT combined with DWT based watermarking algorithm to watermark the encrypted image were proposed which increases robustness of the watermark. These method embeds the binary watermark in encrypted image and decryption is done after extraction of watermark.

N.V.S. SreeRathna Lakshmi [13] introduced A Novel Steganalytic Algorithm based on III Level DWT with Energy as Feature. SVM classifier is employed over here, to classify between the images. a steganalytic algorithm that detects the stego/normal image with 90% accuracy. The accuracy rate remains stable when different sets of images are tested.

Ali and Fawzi [14] proposed a modified high-capacity image steganography technique that depends on wavelet transform with acceptable levels of imperceptibility and distortion in the cover image and high level of overall security. The basic decomposition step for images using the 2D Wavelet transform. Also, different levels of Wavelet transform were tried in that paper.

CONCLUSION

Here we conclude from this review paper transform domain provide robustness,capacity and security in fingerprint steganography. Most of time use Haar Discrete Wavelet Transform to hide message.Idea of improvement for Fingerprint based steganography to increase a level of 2-D DWT. Level of 2- D DWT provide more capacity and robustness. DWT provide more robustness and capacity than DCT.

REFERENCES

1. Rajlaxmi Chouhan*, Agya Mishra**, Pritee Khanna***, "Fingerprint Authentication by Wavelet-based Digital Watermarking", International Journal of Electrical and Computer Engineering (IJECE) Vol.2, No.4, August 2012.
2. Ameya K. Naik, Raghunath S. Holambe, "A Blind DCT Domain Digital Watermarking for Biometric Authentication", International Journal of Computer Applications (0975 - 8887)Volume 1 – No. 16,2010
3. Cameron Whitelam, Nnamdi Osia and Thirimachos Bourlai, "Securing Multimodal Biometric Data through Watermarking and Steganography", IEEE,2013.
4. Mohammed Alkhathami, Fengling Han and Ron Van Schyndel ,"Fingerprint Image Protection Using Two Watermarks Without Corrupting Minutiae", IEEE,2013.
5. Mohammed Alkhathami, Fengling Han and Ron Van Schyndel, "Fingerprint Image Watermarking Approach Using DTCWT without Corrupting Minutiae, 6th International Congress on Image and Signal Processing (CISP 2013).
6. Khalil Zebbiche, Lahouari Ghouti, Fouad Khelifi and Ahmed Bouridane, "Protecting Fingerprint Data using Watermarking", IEEE , 2006.
7. Ani1 K. Jain, Umut Uludag and Rein-Lien Hsu, "Hiding a Face in a Fingerprint Image", IEEE , 2002.
8. Yung-Kuan Chan a, Wen-Tang Chen b, Shyr-Shen Yu b,*, Yu-An Ho b, Chwei-Shyong Tsai a, Yen-Ping Chuc ,"A HDWT-based reversible data hiding method", Elsevier, 2008.
9. Vikas pratap singh, Prof. Shrikant lade "HAAR WAVELET DOMAIN ANALYSIS OF IMAGE STEGANOGRAPHY", International Journal of Technical Research and Applications, Volume 1, Issue 5 (Nov-Dec 2013).
10. Mayank Vasta, Richa Singh, Afzel Noore*," Improving biometric recognition accuracy and robustness using DWT and SVM Watermarking" IEICE Electronics Express, 2005.
11. Mayank Vasta, Richa Singh, Afzel Noore*,Max M. Houck**,and Keith Morris," Robust biometric image watermarking for fingerprint and face template protection", IEICE Electronics Express,2006.
12. V.Chandra Prasad, S.Maheswari." ROBUST WATERMARKING OF AES ENCRYPTED IMAGES FOR DRM SYSTEMS", IEEE,2013.
13. N.V.S. SreeRathna Lakshmi," A Novel Steganalytic Algorithm based on III Level DWT with Energy as Feature", Research Journal of Applied Sciences, Engineering and Technology, May 15, 2014.
14. Ali Al-Ataby and Fawzi Al-Naima," A Modified High Capacity Image Steganography Technique Based on Wavelet Transform" The International Arab Journal of Information Technology, Vol. 7, No. 4, October 2010.