REVIEW ON FINGERPRINT BASED AUTHENTICATION TECHNIQUES

[1] DEVENDER DHAKED , [2] MANISH MATHURIA

[1] M.Tech Scholar , Dept. of Computer Sciences, MACERC, Jaipur
[2] Assistant Professor, Dept. of Computer Sciences, MACERC, Jaipu

Devenderdhaked003@gmail.com, Manishmathuria@outlook.com

Abstract: **— Traditional digital watermarking scheme uses an arbitrary digital pattern as the watermark which has limitations in proving ownership of the watermark. The issue of ownership watermark is addressed. The bio-metric pattern of fingerprint is used to generate the digital watermark that has a stamp of ownership. The generated watermark has been studied for uniqueness and identification and has been used to watermark digital images. In this paper discuss about the watermarking of a fingerprinting based to prevent the forgery users and also discuss the concept of a watermarking. In this paper enhancement process of a fingerprint like, binary thinning process, minutiae process etc. Also, discuss the techniques of a watermarking i.e. spatial domain and the frequency domain and also further divided into techniques process like a least significant bit(LSB), discrete wavelet transform etc. and analysis of a DWT based an embedding and Extracting process. To find out the image quality i.e. PSNR is high and the MSE is a low.**

Keywords: **— Fingerprint; Fingerprint Recognition; Fingerprint minutiae; Digital Watermarking; Least Significant Bit (LSB); Discrete Wavelet Transform (DWT).**

I. INTRODUCTION

Fingerprinting is biometric terms depend on an assurance system benefit of a personal identification techniques. It provides the security of unauthorized users. This does not allow an individual, other than the owner, to manipulate, duplicate, or access media information without getting owner's permission. "Digital watermarking" is a technique to protect the copyright data such as document i.e. audio, video, images and so on of a fake person [1]. Biometric Fingerprints are a unique data generally used for personal identification and authentication purpose. But while transmitting over network to serve the request of intelligence agencies in order to use them for identification purposes they may be susceptible to accidental or purpose attacks. It is necessary to conserve loyalty and also the prohibit modifications [2].

Fingerprint recognition has quickly become the generally used technology in biometrics and forensic application. In a crime view, fingerprints play an important role in terms of identification of criminals. Latent prints are very imperative in forensic as they are evidence of interaction between an individual and the surface containing the fingerprint impression [4]. Most importantly, alteration from traditional fingerprint processing may contaminate the evidence and even rule out further evaluation from other perspective. The fingerprints obtained in crime scenes are known as latent fingerprints. Latent fingerprints are either visible or not visible to human naked eye [5]. Forensic investigators use various techniques to make invisible prints visible. However, these techniques rely on adhesives and chemicals to detect, visualize and preserve latent fingerprints on the surfaces [3]. Several administrative, legal, and news organizations depend on the digital images to take major judgments or used as a photographable proof for a particular event.

This digital image shows some difficulties, as the threat of digital images has matched with the prevalent accessibility of image editing software. It is necessary to provide digital images with good contrast and digital is requisite in various major fields, for example, vision, remote sensing & biomedical image investigation. Delivering visually normal images or transforming an image to enhance display the visual information enclosed in the image is a constraint for approximately all vision & image processing strategies. The fingerprint identification is an automated procedure to identify the identity of a person, based on comparison of stored fingerprint images with the input fingerprint images. These are conspicuous bio-metrics, utilized to check on computer systems. The fingerprints are the impressions or patterns that are existing in fingers of human with any age and over the time this pattern never alters [7]. In recent years, the fingerprint identification technique has attracted the interest of so many researchers, due to its several benefits. One of the best benefits is that it is very well acknowledged by the legal community. This identification technique is very

fast, reliable, least cost and easiest way to recognize an individual. Also, this identification technique has been broadly acknowledged for its accurateness in authentication as the probability of identical finger of two different persons is exceptional. Fingerprint never changes until any physical disorder like accidents occurs or those who works in mechanical or metal industries with burning or hot materials which can harm finger prints. Fingerprints are very beneficial [6].

There are two processes of watermark scheme which are embedding and extraction. In the embedding process, watermark is embedded into the multimedia digital data. After the modification data is known as watermarked data. Another process of watermarking is extraction in which watermark is extracted from the watermarked data and original data is found. Then for the security checking, extracted watermark is compared with the original watermark. If both are same the resultant data is authentic otherwise there may be a chance of attack.

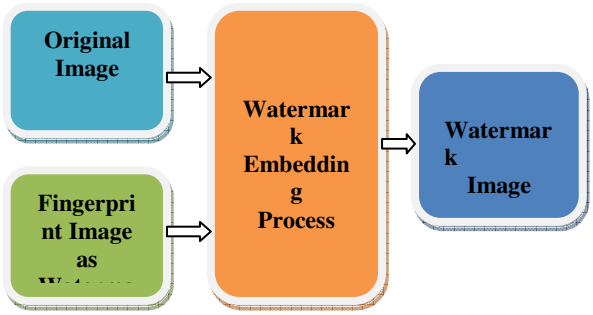

Fig.1 Embedding Method

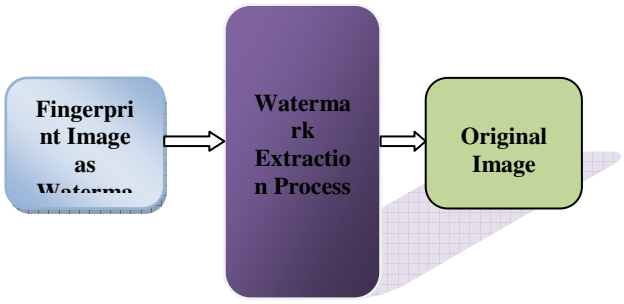

Fig.2 Extraction Method

II. Fingerprint Process

A. Fingerprint minutiae

Fingerprints are the patterns formed on the epidermis of the fingertip. The fingerprint is composed of ridges and valleys. It is one of the best biometric of a minutiae fingerprint. It is mainly used in a criminal record. It is a unique identification of a person because different person of the different fingerprint. Termination and bifurcation are the two feature point of a personal identification [10].

(a) Ridge ending (b) Bifurcation

Fig.3 Types of local ridge features

B. Fingerprint Recognition Process

The process is performing of two phases:

a. Training (Enrollment).

b. Testing (Recognition).

During the training phase each fingerprint is captured by biometrics sensor or reader to generate digital image [12]. Fingerprints are consisting of a combination of ridges & valleys named as patterns. These patterns utilize for authentication by the pattern identification methods. Pattern identification is a best characteristic of the input images as identifying patterns of comprises and the retained relations. The pattern identification methods are classified as Structural & Decision of theoretic. Descriptors Relationships are utilized to define a pattern as the structural method. Whereas, area, length & texture descriptors are utilized to define a pattern in the decision theoretical method. The most significant category of fingerprint identification system is to expose the better descriptors, which are presented in a better way. The fingerprint identification system based on pattern works through creating data of input data images is created [7]. When the input parameters are provided, if these are matched with a database of feature vector & based on the result, authentication is allowed or rejected to the individual [11].

III. Digital Watermarking

Watermarking is a technique to hidden the communication, Digital watermarking is somewhat similar to physical object watermarking, the technique of watermarking is used in digital content not for physical objects. In watermarking a low energy signal is embedded into another signal. In digital watermarking, there are two signals, one is low energy signal and other is main signal. The low energy signals contain some security information and main signal referred to as watermark. The cover signal contains information such as an audio clip, video sequence, still image also text document in digital format.

A. *Types of a watermark*

The bulk of the pictures in the web, utilizes watermark to give validness as a part of terms of including a primary picture which is overlaid on the essential picture, and gives a method for securing picture. The watermark may be of two sorts visible or invisible.

1) Visible watermarking

In visible watermarking a semi transparent visible image is applied to the primary image. In this watermark a signal is changed such that the watermarked signal is totally different from the actual signal, for ex, including a picture as a watermark to another picture. It comprises of logo or seal of the association that permits the saw of essential picture, yet at the same time marks it obviously as the property of the owning association. The watermark doesn't absolutely cloud the essential picture; however, it does distinguish the proprietor and keeps the picture from being utilized without that recognizable proof connected. It is imperative to overlay the watermark in a manner which makes it hard to remove, if the objective of showing property rights is to be accomplished.

2) Invisible watermarking

In invisible watermarking semi straightforward picture which can't be seen, yet can be identified algorithmically. Flags in invisible watermarking don't change, all things considered, i.e., yet in the yield sign reflects just minor varieties. Case in point, in invisible watermark added a few bits to a picture changing just its slightest huge bits. Diverse sorts of invisible watermarks contain distinctive application innovation.

3) Blind watermarking system

A watermarking technique is said to be blind, if to extract the watermark from watermarked data it does not need original image. The blind watermarking system is also known as oblivious. The blind watermarking system is more popular because it decreases the overhead of cost and memory for storing original data.

4) Non –blind watermarking system

It requires the original data to essence the watermark is known as non-blind watermarking system, it is also robust than the blind watermarking system.

B. *Characteristics of digital image watermarking*

There are various main features of digital watermarking:

1) Imperceptibility

The watermark included is intangible both factually and perceptually and don't change the style of mixed media content that is watermarked. In the still pictures watermark doesn't make obvious relics, alter the bit rate of the feature or set up discernible frequencies in sound signs.

2) Robustness

On the premise of use, the digital watermarking method support diverse levels of strength against changes in watermarked picture. In the event that digital watermarking is utilized for possession distinguishing proof, then the watermark must be robust against any alterations. The watermark thought not devastated or corrupted as a consequence of geometric contortions or a malignant sign like simple to advanced transformations, digital to-simple transformation, resembling, trimming, turn, scaling and pressure of the substance. Whereas though it is utilized as a part of substance validation, the watermark ought to get demolished because of the delicacy and if the substance gets changed that can be effortlessly distinguished. In the design of any watermarking scheme, the ability to withstand host data distortions introduced through standard and legitimate data processing is defined as robustness. Standard data processing includes all host data manipulations and modifications that the data might undergo during its distribution chain. [9].

3) Inseparability

After the digital substance is inserted with watermark, isolating the substance from the watermark to recover the first substance is unrealistic.

4) Security

As far as security it keeps unapproved access of clients from distinguishing and adjusting the embedded watermark in the spread sign. Watermark keys give certification that an unapproved client never ready to recognize/adjust the watermark. Regardless of the data type, we have identified a few challenges for watermark security herein. Firstly, the separation between watermark security and watermark robustness can be very well-defined. Security is the watermark resistance against any intentional attempt by an adversary to impair watermark detection, as opposed to the normal data processing that a robust watermark should survive. This isolation assumes that the intention behind every operation is known and deterministic. In a real scenario, an innocent-looking operation might compromise the watermark usability, but one may not necessarily be able to say whether it is deliberate or not [9].

5) Capacity

Data capacity refers to the amount of information one can embed into any single piece of data. A watermark that encodes n bits, can embed 2n different messages and is referred to as multiple

bit watermarking. In contrast, a zero bit watermark carries no hidden message, which means only the presence/absence of a watermark can be investigated. Also, capacity is sometimes given relative to the size of the host data. For instance, the capacity of a watermarked video can be measured by number of embedded bits per frame. Some other references, consider the number of correctly retrieved bits as the watermark capacity.

IV. Enhancement Techniques

The enhancements techniques have been broadly categorized as: spatial domain based and frequency domain based.

A. Spatial domain method

This technique is directly embedded to the pixel value of an image. Gray level image and the color image both the use of a spatial domain method. It is a less robust than the frequency domain method. It is also a low computational tool. It is also a lossless compression of an image. For lossy compression schemes like JPEG, some of the message bits get lost during the compression step.

1) Least significant bit

For hiding information within the images, the LSB (Least Significant Byte) technique is usually used. To a PC a picture document is essentially a record that shows diverse hues and intensities of light on distinctive zones of a picture. It is an 8 bit digit is used into the original image to protect the unwanted users. Basic method of data hiding in an image is given as-:

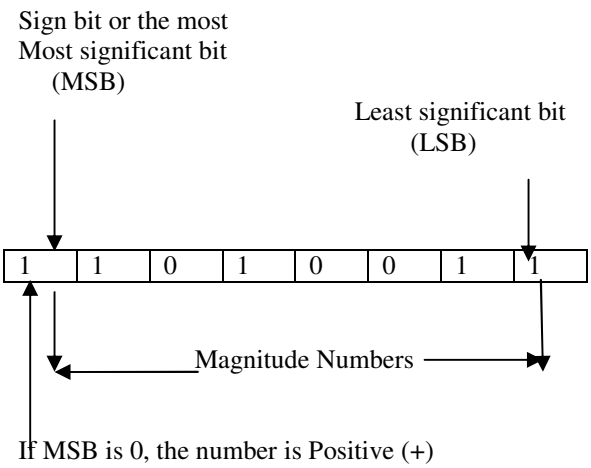

Fig.4 Least Significant Bit

B. Frequency domain method

Here we can implant watermark in DCT, DFT, FFT spaces and so forth. The primary quality offered by change area procedures is that they can exploit properties of exchange spaces to address the restrictions of pixel-based systems or to support extra components. A possible disadvantage of spatial procedures is that they are not exceptionally hearty against attacks. Notwithstanding this, adaptive watermarking strategies are some more troublesome in the spatial space. Both the robustness and quality of the watermark could be enhanced if the properties of the spread picture could also be misused. For example, it is by and large desirable over conceal watermarking data in loud districts and edges of the pictures, somewhat then in smoother areas. The advantage is twofold; Degradation in smoother locales of a picture is more noticeable to the HVS, and turns into a prime focus for lossy compression plans. Bring these perspectives, working in a frequency space or something to that affect turns out to be exceptionally appealing.

1) Discrete wavelet transforms

In Wavelet theory is usually utilized in the signal processing. But, then the traditional wavelet transformation displayed some restrictions on the 2-D image processing. The image processing technique is a collectively partial differential equation & the wavelet theory can perform in a better way by holding the information of the image edge. This wavelet transform method can be utilized on the fingerprint patter to carry out the authentication. Wavelets are helping to cut down the input data images into various frequency components. Then every element is observed with a determination method of scale. The fingerprint images are divided by utilizing discrete wavelet transform in the wavelet based approach. Three stages of decomposition of fingerprint images are executed for the purpose of training. In the time of the decomposition procedure mean & standard deviation is utilized. To classify these fingerprint patterns, that are rotated from 0 to 360 degrees & also every step is increased by 10 degrees. After that, a set of values of wavelet statistic and co-occurrence feature are defined. It can be clearly stated that the directional resolving power of wavelets mines, texture information in LL, LH, HL & HH diagonal directions. Image preprocessing of finger printing or post processing are not required in wavelet based fingerprint recognition systems. Wavelet based pattern recognition technique are fast enough in contrast to minutiae based method. Another one benefit of the wavelet is that it performs at the least three levels of texture splits that make an automatic fingerprint identification system perfect. This is the drawback of texture analysis systems because the images are observed at a single scale [4]. It split up into the two parts, first is high frequency and another is low frequency. This process is continuing until the signal has been entirely decomposed or stopped before by the application at hand. For compression and watermarking applications, generally no more than four decomposition steps are computed.

Wavelet transform is both time-frequency domain combined analysis method. Its main feature

is multi-resolution analysis. The DWT divides the input image into four Sub-images which are non-overlapping multi-resolution sub bands LL, LH, HL and HH. The LL sub-band represents the coarse-scale (approximation) DWT coefficients and the three LH, HL and HH sub-band represent the fine-scale (detail) coefficients of DWT. Because of excellent spatial frequency localization properties of DWT, the DWT are useful to identify the region in host image where a watermark can be embedded effectively.[10]

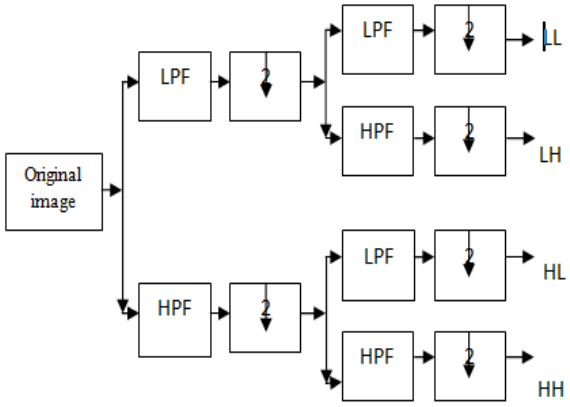

Fig.5 Discrete Wavelet Transform

C. Parameters

The parameters PSNR, MSE, Accuracy, FMR and FRR are as follows**.**

1) Calculate Mean Square Error (MSE) value of watermarked and cover image. Where x is cover image, x^ is watermarked image, N is the size of cover image.

2) Calculate Peak Signal Noise Ratio (PSNR) value of watermarked and cover image. Where m is the maximum value of the cover image

3) False Matching Rate

It is the probability that the system will decide to allow access to an (FMR) imposter

V. Literature Survey

[8] This paper uses the major challenges of the Automatic Finger print Recognition System. This paper uses the filter technique to remove the blur and the noise of a salt and pepper and also a Gaussian noise. This paper is calculated to the PSNR and a MSE value for a result analysis. This paper work to the various type of the enhancement technique. The experimental result shows that the feature of an image enhancement and to check the quality of the image likes ridge and valley. Also, in this paper is used to the latent image and it is extracted fingerprint from FVC2004.

[6] This paper uses the fingerprint identification for a person unique in recent years. It is the concept of a biometric system. This paper improve the technology of a fingerprint is used to the various type of the fingerprint image. It is the biometric technique used to prevent the copyright data. There are the different approach used as pattern recognition, wavelet etc .Wave atom is one of the best new geometric multi scale multidirectional transform that is suitable for the representation of the fingerprint structures. Fingerprint recognition is used as minutiae based method. It is also provides the accuracy and the robustness of this fingerprint concept. With compare to other existing method, Wave Atom Transform and Modified Cuckoo Search (MCS) algorithm provides the better results of a PSNR value.

VI. Conclusion

In this paper discussed, different enhancement techniques is used for the concept of a fingerprint based watermarking and also discuss the digital watermarking method DWT, which provide the more secure and robustness in watermarking is also get. So to conclude, watermarking is adding "ownership" information in multimedia content to prove the authentication. In this technology a data or unperceivable digital code (watermark), carrying information about the copyright status of the work to be protected. Today, digital data security covers different topics as access control, authentication, and copyright protection for multimedia data like: Image, audio, video and multimedia products. The possibilities came into existence when invisibilities of QR-code image like to be a full security features.

Many the researches were found on digital watermarking using DWT. Watermarking of gray scale image is researched by many researches but the watermarking of color image is still required for future processes for an enhancement the good quality image.

References

[1]. Ms.Jalpa M.Pate1, Mr.Prayag Patel, "A brief survey on digital image watermarking techniques". In International Journal for Technological Research in Engineering Volume 1, Issue 7, March-2014 ISSN.

[2]. Dr. Mohammad V. Malakooti, Zahed FerdosPanah, "Image Recognition Method based on Discrete Wavelet Transform (DWT) and Singular Value Decomposition (SVD)" In ISBN: 978-0-9853483-3-5, 2013 SDIWC.

[3]. Sisanda Makinana, "Latent Fingerprint Wavelet Transform Image Enhancement Technique for Optical Coherence Tomography", ISBN: 978-1-4673-9187-0 ©2016 IEEE

[4]. S. Meissner, R. Breithaupt, and E. Koch, "Fingerprint fake detection by optical coherence tomography," in SPIE BiOS. International Society for Optics and Photonics, 2013, pp. 85 713L–85 713L.

[5]. L. R. Cambrea and B. G. Harvey, "Fumeless latent fingerprint detection," Nov. 5 2013, uS Patent 8,574,658.
[6]. Subba Reddy Borra, "A Broad Survey on Fingerprint Recognition Systems", IEEE WiSPNET 2016 conference.
[7]. A1-Ani M. S., "A novel thinning algorithm for fingerprint recognition", International Journal of Engineering Sciences, Feb 2013,Vol. 2, No. 2, pp. 43-48.
[8]. Subiya Zaidi, "To Evaluate the Performance of Fingerprint Enhancement Techniques", IEEE INDICON 2015
[9]. Arezou Soltani Panah, "On the Properties of Non-Media Digital Watermarking: A Review of State of the Art Techniques", in volume 4 IEEE 2016.
[10]. Pooja Chinchmalatpure, "Fingerprint Authentication by hybrid DWT and SVD based Watermarking" , IEEE Sponsored 2nd International Conference on Innovations in Information Embedded and Communication Systems in 2015 IEEE.
[11]. D. Srinivasulu Reddy, Dr. S. Varadarajan, and Dr. M. N. Giri Prasad, "2D-DTDWT base image denoising using hard and soft thresholding", February 2013, Vol. 3, No. 1, pp. 1462-1465.
[12]. Mouad.M.H.Ali, "Fingerprint Recognition for Person Identification and Verification Based on Minutiae Matching", 2016 IEEE 6th International Conference on Advanced Computing.