A Fingerprint Template Protection using Watermarking

Sunil Kumar
Associate Professor
HCTM Technical Campus,
Kaithal (Haryana) India

Garima
M.Tech. Scholar
HCTM Technical Campus,
Kaithal (Haryana) India

Aditi Garg
M.Tech. Scholar
Dcrust University,
Murthal(Haryana) India

ABSTRACT
This paper presents a watermarking technique for fingerprint images using the DWT-SVD (Discrete WaveletTransform - Singular Value Decomposition). The watermarking image is embedded and extracted to calculated the PSNR (Peak Signal to Noise Ratio) and NC (Normalized cross correlation) value. Watermark Embedding Technique or the algorithm should be imperceptible i.e. embedding watermark should not affect the quality of original image but can be improved the quality of image. MSE (Mean Squared Error), PSNR (Peak Signal to Noise Ratio) between the original host image and the corresponding watermarked image to calculate of the superiority of a watermark embedded images and NC (Normalization co-relation) is calculated between Watermark images and extracted watermarked to the superiority of a watermark extracted images. Watermark should be robustly embedded into image which remains in fact after any type of image processing. This research work will be to present highly imperceptible & robust. Images watermark embedding and extraction technique. The DWT-SVD (Discrete WaveletTransform -Singular Value Decomposition) domain is used to embed the watermark data into fingerprint images and Singular Value Decomposition (SVD) is used to transform the image in this technique are going to present a watermarking algorithm with the combination of images.

Keywords
DWT-SVD, Watermarking Image, Embedding, Extraction, Fingerprint Image

1. INTRODUCTION
A watermarking technique is used for fingerprint images using the Discrete WaveletTransform -Singular Value Decomposition (DWT-SVD). Generate a combined minutiae template containing minutiae features of each of the two Fingerprints captured in enrolment phase and stored in a database. In the authentication process, a two-stage fingerprint matching process is proposed for matching the two query fingerprints against the enrolled template. Reconstruct a fingerprint look like image from combined minutiae template. In this Fingerprint images, user identity is combined with a biometric identification during the authentication process. The user identity consists of name and its id (identification). It is encoded using the MD5 hash function to verify the data integrity. MD5 is a secure 128-bit hash function, so it can't be possible to obtain a user identification number based on the hash value and it is infeasible to change a message without modifying its hash value. The hash value is that converted into binary value and then converted into a watermarked image of size 256x256, equal to the size of the fingerprint image. The DWT-SVD (Discrete WaveletTransform -Singular Value Decomposition) domain is used to embed the watermark data into fingerprint images. DWT-SVD removes the directionality and shift variance problems present in the wavelet transforms by using complex basis functions. For decomposition purposes, DWT-SVD uses directional filters [1].The algorithm comprises the following steps:-

- The User information that identify the user, encode the MD5 hash function
- Convert the hash value of binary image to construct the water-marked image.
- DWT-SVD performed on both fingerprint images and water-marked images up to 4 levels on watermarking technique.
- In multiplicative fusion rule using to combine the fingerprint image and watermarked image.
- Apply the inverse DWT-SVD to obtain watermarked images.

Watermark Embedding Technique or the algorithm should be imperceptible i.e. embedding watermark should not affect the quality of original image. MSE (Mean Squared Error) and PSNR (Peak Signal to Noise Ratio) is calculated between the original image and the corresponding watermarked image to calculate of the superiority of a watermark embedded images. Watermark should be robustly embedded into image which remains in fact after any type of image processing. The added watermark images information should not be removed beyond reliable detection i.e. watermarking technique should be as secure as possible. It should consume less time for watermarking [2].

2. RELATED WORK
Bhatnagar and Raman 2009 [3] performed work; "A new robust reference watermarking scheme based on DWT-SVD" This paper represent the novel semi blind watermarking technique based on SVD (singular value decomposition) and DWT (discrete wavelet transform) for validity and security. They used a gray level emblem picture as watermark instead of arbitrarily generated Gaussian noise kind watermark. To insert the watermark the original picture is altered into wavelet field and an oriented sub-image is produced by means of directive contrast and wavelet coefficients. Embedding of watermark into reference image was performed by changing the SVD of reference picture by means of the SVD of the watermark image. They also developed a scheme for the drawing out the watermark image from faint picture.

Yasunori *et al.*2009 [4]performed work; represent a planned a watermark embedding technique for image copyright protection based on Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT) and Singular Value Decomposition (SVD). It has a high-quality presentation on imperceptibility and strength against attacks to trial clears. That is mainly because they only apply SVD to a 32 X 32 matrix compared with the SVD method is 512 X 512 and the DCT+SVD method value 64 X 64 which uses 4 times more DCT than our method. Besides, it also saves lots of memory

space. These are very important features for some environment that lack of resources such as mobile phone and other embedded systems.

Ramakrishnan*et al.*2011 [6] performed work; represent the projected of watermark embedding technique using a mixed image which satisfies together imperceptibility and toughness necessities. They used SVD of vertical and diagonal details of Wavelet Transformation to insert watermark image. Additional to boost and the watermark image manage the power, scaling factor was used. Investigational consequences were described in requisites of cross correlation (CC), Peak signal to noise ratio (PSNR), and gain factor to reveal the efficiency of the planned method. The projected method can efficiently oppose ordinary picture dispensation attacks, particularly by low pass filtering and JPEG compression.

Rajani and Ramashri 2013 [5] performed work; represent to develop a mixture of SVD (Singular Value Decomposition) and DCT (Discrete Cosine Transform) frequency by hybrid watermarking algorithm domains and Canny Edge detector. A Non-blind watermarking technique is the projected technique. By means of Singular Value Decomposition (SVD) the toughness of the technique can be improved. By incorporating edge detector imperceptibility of the watermark image can be improved. The projected technique is extra safe and strong to a variety of operations like compression attack, histogram equalization, scaling, cropping attack, rotation attack, salt & pepper noise attack, and filtering attack.

Van Schyndel *et al.*2013 [7]performed work; represent as using a watermarking algorithm used as the fingerprint image protection without corrupting minutiae points. This method a watermark images into a fingerprint image can be embedded using the DCT technique. This idea behind its method for the watermark is embedded into the DCT blocks which contain two minutiae points or less. The template and the host fingerprint are exactly used the same image. By comparing the total number of minutiae points the watermark effect is determined by before and after watermark embedding.

3. PROPOSED WORK

In this proposed work, the dual Level watermarking image transformed domain is proposed. The watermarking image is based on DWT-SVD (Discrete WaveletTransform -Singular Value Decomposition) is used to transform the image. It is encoded using the MD5 hash function which work on a different hash value. MD5 is message digest algorithm that used to protect the data integrity of media to detect changes. MD5 is one way hash function that utilized a wide variety of cryptographic applications, and used to verify the data integrity. The hash function is converted the binary image into watermarked image size 256 x 256 equal the size of fingerprint Image. The Discrete WaveletTransform -Singular Value Decomposition domain is used to embed the watermarked image into fingerprint images. DWT-SVD is digital watermarking technique that is applied on fingerprint images as using the host image is chosen to embed the watermarking because the information of host image is in high frequency. DWT-SVD uses directional filters by using decomposition purposes. These filters are able to extract the images, such as watermarked, even after the host image has been embedded into the watermarked image. Multiplicative fusion is used to distribute the watermark evenly to whole fingerprint image, including the real parts and imaginary parts, without affecting the information present in the fingerprint image. In this proposed model, the watermarking is divided into two parts are embedding and extraction work.

The Watermarked image to embed the host image is calculated the PSNR value and the other Watermarked image to extract the watermarked image to calculated the NC value. The watermarking algorithm creating some steps:-

- Generate the hash value of user information using MD5 hash function.
- The hash value is converted into binary form to construct the watermarked image.
- The fingerprint and watermarked image is decompose by the Discrete WaveletTransform - Singular Value Decomposition
- The multiplicative fusion rule is applied and Combine on the watermark and fingerprint image.

Apply the inverse DWT-SVD to obtain the watermarked image.

3.1 Watermarking Algorithm

First of all, The DWT-SVD model is performed on both the fingerprint image and watermarked images up to four levels. At each level, DWT-SVD model are sorted according to their in ascending order. To collect the user information to identify the image and encoded the hash value as using MD5. MD5 is one way hash function that utilized a wide variety of cryptographic applications, and used to verify the data integrity. The hash function is converted the binary image into watermarked image size 256 x 256 equal the size of fingerprint Image. The watermark image is usually a black and white image. Nowthe DWT-SVD model is performed on both the images as using host and watermarked using over the 4 levels. The multiplicative fusion rule is apply and combine the host image and watermarking image. Multiplicative fusion is used to distribute the watermark evenly to whole image, including the real parts and imaginary parts, without affecting the information present in the fingerprint image. To obtain the watermarked image and Apply the inverse DWT-SVD. Inverse wavelet transform is performed to reconstruct the watermarked image.

The embedding and extraction of watermarked is done with the help of DWT-SVD (Discrete WaveletTransform -Singular Value Decomposition) along with their Fingerprint template protection using watermarking.

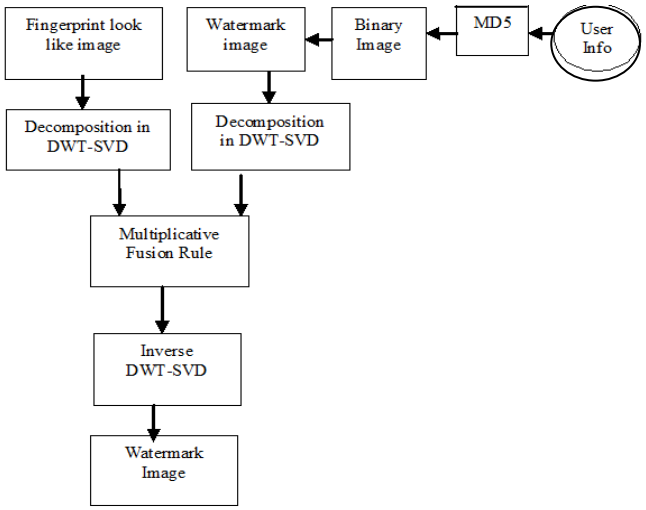

Figure 1: The block diagram of proposed embedding watermarking process.

3.2 Watermark Embedding Algoritm

The goal of Embedding process is embed the watermark in the DWT-SVD.

Step1: Read original host image.

Step2: Apply DWT-SVD to the original image and get edges of host image and consider it as watermark image.

Step3: Read a watermark image and rescale it as according to the size of the original image.

Step4: Separate the layer of original image.

Step5: Apply DWT- SVD on layer of image and get all singular values matrix.

Step6: Addwatermark images to the singular values matrix A.

3.3 Watermark Extraction Algorithm

To extract the watermark image, the following processes are applied

Step1: Read the template image and watermarked image using DWT-SVD.

Step2: On the watermarked image to Apply the attacks.

Step3: Separate the layers of watermarked image to get the watermarked layers.

Step4: Apply the DWT- SVD on watermarked layer to extract watermark image.

Step5: To compute the matrix which contain the watermark image and obtain watermarked co-efficient.

Step6: Perform inverse DWT-SVD images to obtain the watermarked and Extract the Watermark "A" image obtained from step 5 using it.

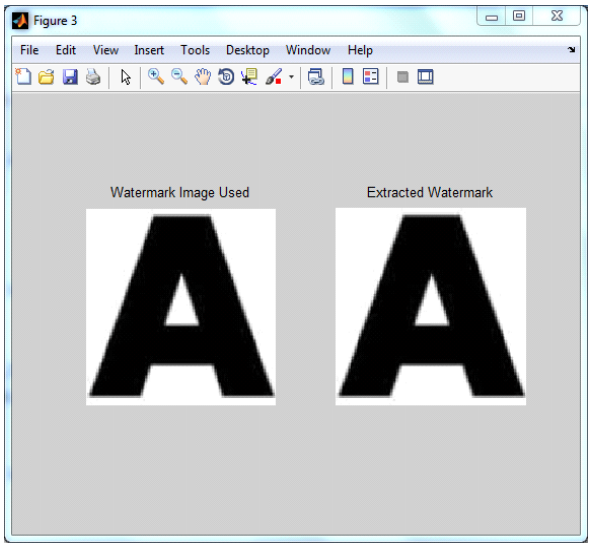

Figure 2: Diagram of Proposed Watermark Extraction Process

4. RESULTS

The proposed watermarking perform technique is evaluated using "Lena" image with their 256 x 256 size of image is implemented and experiments are conducted for watermark embedding and extraction images using MATLAB 7.10.0 version. The performance of the presented image watermarking algorithm is evaluated on the basis of Imperceptibility, complexity, security, embedding, extraction, dynamic scaling and robustness. The Robustness of watermarking technique to calculated the PSNR value (peak to noise ratio) which is compare on original host image and watermarked on host image. To calculated the quality like NC (Normalized cross correlation) is used to find correlation between watermarked and extract watermarked. The NC value is closer to 0-1 has maximum value be defined, it is possibly increase the robustness of watermarked technique and PSNR value is calculated the embedded watermarked of robustness and imperceptibility of watermarked "Lena" image. NC is used to find correlation between "watermarked image" and "extracted watermarked".

Here results are discussed for "Lena" image as original host image. The grayscale image "Lena" is of size 256 x 256. The original host "Lena" image as input image to extract the watermark image "A" shown in Figure 2 and create a new output is a watermarked image as defined. The edge image is calculated from the "Lena" image and is acted as watermark image and both the images are embedded using SVD.

(a)Original image (b) Watermarked image

Figure 3: Original Image (a) and Watermarked image (b)

4.1 Mean Squared Error (MSE)

To determine the resemblance between the real image and equivalent watermarked image an inaccuracy is calculated by subtracting the watermarked image pixel intensity values from the actual image pixel intensity values, and after that calculating the mean of the in accurate signal.

$$MSE = \frac{1}{MN}\sum_{i=0}^{M}\sum_{i=0}^{N}(x(i,j) - y(i,j))2$$

Where i and j are the pixel positions of the image having M number of rows & N number of columns and *x (i, j)* is the pixel intensity values of actual image and *y* (*i, j*) is the pixel intensity values of corresponding watermarked image. Mean Squared Error is zero when pixel value both images are same.

4.2 Peak Signal to Noise Ratio (PSNR)

The units of Peak Signal to Noise Ratio are decibels and it is inversely relative to the MSE (Mean Squared Error). It is specified by means of the equation:

PSNR-Value = 10 * log 10 (255^2 / mse1);

Larger the cost of Peak Signal to Noise Ratio (PSNR) better is the value of the watermarked image.

4.3 Performance

To this algorithm demonstrate the planned imperceptible, work of the watermarked image embedded and extraction to Calculated the NC (Normalized Correlation) and PSNR (Peak Signal to Noise Ratio) value is computed using for watermarked image. Figure shows bar graph of PSNR between the value of existing and proposed model of original

host image "Lena" as shown in figure 3(a) and corresponding watermarked image as shown in figure 3(b) and the figure 4 and figure 5 shows the bar graph of NC between the value of existing and proposed model. The approaches of PNSR and NC values of existing models are difference between the existing value of PNSR is 37.156 and the NC value of existing value is o.963 and the other approach of proposed model the PSNR value is 39.1 and then improved extracted the watermarked image NC value of proposed model is 1 as defined in figure 5. The values for these parameters for various original & watermark images are tabulated defined in table 1. Higher values of NC improved the PNSR proposed value smaller values of NC prove the high imperceptibility of proposed algorithm. The table shows that the quality measure the value of PSNR between the host image and watermarked host image and NC between the watermarked and extracted watermarked on existing and proposed model. After applying the Existing and Proposed on watermarking "Lena" image prove that the proposed watermarking technique is robust against watermarked attack.

Table 1: Host Image watermark "Lena" with Attack.

Approach	PSNR	NC
Existing	37.156	0.963
Proposed	39.1	1

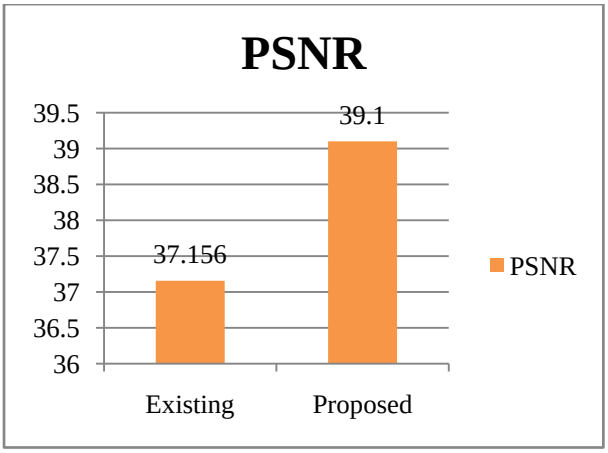

Figure 4 :Proposed and Existing Model of PSNR value

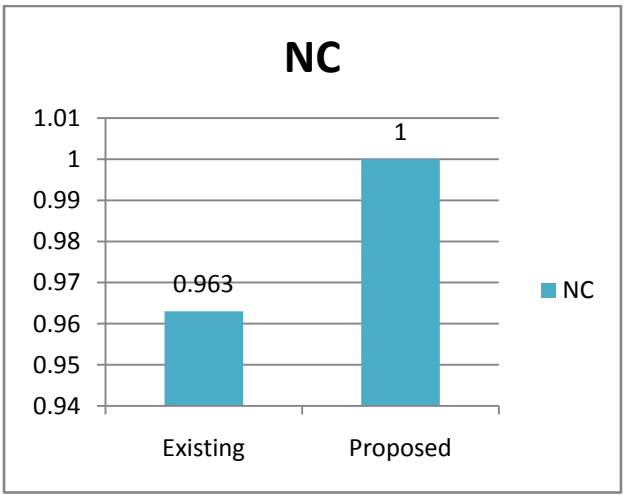

Figure 5: Proposed and Existing Model of NC value

4.4 Robustness Performance

Similarity between the original watermarks image and the extracted watermarks from the watermarked image is measured by computing correlation using the MSE, PSNR, and NC. The quality measure value of MSE, PSNR, NC between host image and watermarked host image.Original watermarks and extracted watermarks from the watermarked "A" image are shown in figure 2.The robustness of watermarking technique measure by PSNR value (peak to noise ratio) which is compare on original host image and watermarked on host image. To measure the quality like NC (Normalized cross correlation) is used to find correlation between watermarked and original host image. The NC value is closer to 1, it is possibly increase the robustness of watermarked technique and PSNR value is calculated of robustness and imperceptibility of watermarked "Lena" image. NC is used to find correlation between original watermarked image and extracted watermarked image "A".

5. CONCLUSION

A research work has been performed of a new watermarking algorithm for fingerprint image using the DWT-SVD is proposed. Various existing fingerprint image and watermarking techniques are studied in this literature review of the report. Although the maximum techniques are robust to the digital signal processing on watermarking, still these techniques are not secure. So this research work, the proposed model adds the authorization process to authentication factor by combine user identity with biometric methods. In proposed algorithm, one of the watermarks used is binary watermark and other is grayscale watermark. The watermark is embedded into fingerprint image that work in imaginary and real images. To Embedded the Watermark are not affected by fingerprint features. The matching result shown that fingerprint feature after matching the template and watermark "Lena" images to work in calculated the proposed and their existing model.

The algorithm is computed in terms of security, and robustness. To compute the imperceptibility of algorithm PSNR and NC are calculated as in proposed and existing model. The computed values of the parameters show that a highly imperceptible, more secure, and highly robust method of image watermarking.

6. REFERENCES

[1] K V. Reshma *, A.T.Nair and T.Babu, "Identity of User Thrashing and Privacy Protection of Fingerprints" International Conference on Information and Communication Technologies (ICICT 2014).

[2] R. Borisagar and Thanki "compressive sensing based multiple watermarking technique for template protection" , I.J Image , Graphic singnal processing 2015

[3] G. Bhatnagar and B. Raman, "A new robust reference watermarking scheme based on DWT-SVD", Computer Standards & Interfaces (2009), Volume 31, No. 5,pp: 1-6, Sept. 2009.

[4] G.Bhatnagarl and R.Balasubramanian,"Robust Watermarking in Multiresolution Walsh-Hadamard Transform", International Advance Computing Conference (IACC 2009), pp: 894-899, Patiala, India, March 2009

[5] T. RamashriandRajani, "Image Watermarking Algorithm using DCT, SVD and Edge Detection Technique",

International Journal of Engineering Research and Applications, Volume 1, No. 4, pp: 1828-1834,2013

[6] S.Ramakrishnan, T.Gopalakrishnan, K.Balasamy, "SVD Based Robust Digital Watermarking For Still Images Using Wavelet Transform", D.C. Wyld, et al. (Eds): CCSEA 2011, CS & IT 02, pp: 155–167, Tamil Nadu, India, 2011.

[7] M.Alkhathami, F.Han and R.V.Schyndel, "Fingerprint Image Watermarking Approach Using DTCWT without Corrupting Minutiae", 6rd International Congress on Image and Signal Processing 2013 (CCISP 2013).