TELKOMNIKA, Vol.15, No.3, September 2017, pp. 1368~ 1379
ISSN: 1693-6930, accredited **A** by DIKTI, Decree No: 58/DIKTI/Kep/2013
DOI: 10.12928/TELKOMNIKA.v15i3.6437

Using SVD and DWT Based Steganography to Enhance the Security of Watermarked Fingerprint Images

Mandy Douglas[1], Karen Bailey[2], Mark Leeney[3], Kevin Curran[4]
[1,2,3]Institute of Technology, Letterkenny, Co. Donegal, Ireland
[4]Faculty of Computing and Engineering, Ulster University, Northern Ireland
*Corresponding author, e-mail: mandy.douglas@lyit.ie[1], kj.curran@ulster.ac.uk[2]

Abstract

Watermarking is the process of embedding information into a carrier file for the protection of ownership/copyright of digital media, whilst steganography is the art of hiding information. This paper presents, a hybrid steganographic watermarking algorithm based on Discrete Wavelet Transform (DWT) and Singular Value Decomposition (SVD) transforms in order to enhance the security of digital fingerprint images. A facial watermark is embedded into fingerprint image using a method of singular value replacement. First, the DWT is used to decompose the fingerprint image from the spatial domain to the frequency domain and then the facial watermark is embedded in singular values (SV's) obtained by application of SVD. In addition, the original fingerprint image is not required to extract the watermark. Experimental results provided demonstrate the methods robustness to image degradation and common signal processing attacks, such as histogram and filtering, noise addition, JPEG and JPEG2000 compression with various levels of quality.

Keywords: *watermarking, steganography, security, biometrics*

1. Introduction

Biometric systems allow for convenient identification to take place based on a person's physical or behavioural characteristics. Biometric procedures have evolved rapidly in the past decade and are used in many different areas, such as banking and government agencies, retail sales, law enforcement, health services, and airport/border controls [1]. One of the main reasons that these biometric mechanisms are gaining popularity is because of their ability to distinguish between an authorized user and a deceptive one [2]. At present, fingerprint biometrics are said to be the most common mechanism, as these are convenient to use, and cheaper to maintain in comparison to other systems. However, as the development of these applications continues to expand, the matter of security and confidentiality cannot be ignored. The security and integrity of biometric data presents a major challenge, as many benefits of biometrics may quite easily become impediment. Thus, from the point of view of promoting the extensive usage of biometric techniques, the necessity of safeguarding biometric data, in particular fingerprint data becomes crucial [3]. For example, fingerprint biometric systems contain sensitive information such as minutia points which is used to uniquely identify a fingerprint. The use of latent fingerprints is one way that an unauthorized user can access a system. A latent fingerprint can be easily collected as people leave latent prints when they touch hard surfaces. If an unauthorized user was successful in retrieving a latent print it may enable him/her to gain access to the system hence potentially endanger the privacy of users. Additionally, stolen data may be used for illegal purposes, such as identity theft, forgery or fraud. Therefore, increased security of the data is critical [4].

Information hiding techniques like watermarking and steganography can add to the security of biometric systems. Watermarking is a process of embedding information into a carrier file in order to secure copyright, typically ownership. Watermarks can be either visible or nonvisible to the human eye. Steganography is the process of hiding critical data (i.e. identity pin) in a trusted carrier medium (i.e. digital fingerprint image) without third parties sharing any awareness that the information exists. Both methods of information hiding are closely connected [5]. Over the past number of years, many image-based steganography methods

Received May 11, 2017; Revised August 2, 2017; Accepted August 20, 2017

have been broadly classified depending upon the domain as spatial domain steganography and frequency domain steganography. In Spatial domain steganography, methods such as correlation based techniques and LSB substitution, which will be explained later, have been developed and tested. Frequency domain steganography methods consist of many different domains, such as Discrete Cosine Transform (DCT) domain, Discrete Fourier Transform (DFT) domain, Discrete Wavelet Transform (DWT) domain, Singular Value Decomposition (SVD), etc. These techniques are discussed in detail in later sections. Frequency domain methods are considered to be more robust than that of spatial domain methods [6]. Frequency domain methods have been used in combination with other techniques, this approach is known as hybrid steganography. Many of these hybrid techniques make use of a mathematical decomposition called the Singular Value Decomposition. SVD is considered to be one of the most valuable numerical analysis tools available, mainly because singular values obtain inherent algebraic properties and provide stability that permits secret data to be hidden without degrading the perceptual quality of an image [7]. In this study, a wavelet based watermarking algorithm is proposed to enhance the security of fingerprint images. The algorithm embeds secret data into a fingerprint image based on Discrete Wavelet Transform (DWT) and Singular Value Decomposition (SVD). The fingerprint image is first converted to the frequency domain and the SVD is applied on both the original fingerprint image and the watermark image. The singular values (SV's) of the fingerprint image are then modified with the singular values (SV's) of the secret image.

2. A secure Fingerprint Recognition System

Data hiding algorithms are generally based on either substitution or quantisation procedure, and pixel bits or coefficients are manipulated in order to conceal data. Research shows that many frequency domain algorithms exceed that of the spatial domain. However, spatial domain techniques do possess some advantages over frequency domains, for instance, its large capacity to hide data. Nonetheless, the negative points of embedding in the spatial domain, such as its poor robustness to attacks, outweigh the positive ones. Even though, the majority of methods mentioned in the literature review suggest that frequency domain methods are deemed a more appropriate method, disadvantages also exist. In frequency domain embedding the capacity for hiding data is much less than that of the spatial domain. For instance, using DWT as an example, and a bitmap image size 512x512, which is decomposed at first level (i.e. LL, LH, HL, HH), the maximum message or watermark size would be 256x256. Moreover if decomposed further (i.e. LL1, LH1, HL1, HH1), the maximum message or watermark size would be 128x128. Furthermore, depending on how and where the data is hidden, applying compression on the image may cause the hidden message or watermark to be badly distorted or unreadable. When an image is compressed most of the energy stored in the high frequency sub-bands are removed, so if a message or watermark is hidden in these sub bands it may be lost. [8] proposed a method to exploit the wavelet domain by hiding information (watermark image) in the sub-band coefficients of the mid frequency band of an image to produce a stego image. Image quality tests carried out showed positive results. However, after testing the algorithms robustness against jpeg compression, results proved disappointing. Although the results against compression in [9] were unsatisfactory, it is important to note that many other proposed methods based on wavelet embedding have shown encouraging outcomes against compression attacks [9]. It is also important to highlight that loss of hidden data may greatly depend upon where data is concealed in the first place. For example, the low frequency sub-bands (LL) contain the majority of image energy which makes up an image, therefore when compression is applied; most of this information is kept intact. So, if data is embedded in low frequency sub-band the probability of it surviving compression is high. Nevertheless, embedding in low sub-bands can degrade image quality and thus lead to unwanted attention from attacker. On the other hand, embedding data in the higher frequency coefficients have a greater expectancy of data loss after compression is applied, as information contained within higher sub-bands only hold small amounts of image information, most of which is disregarding during compression. It is clear, that determining the correct hiding locations here is critical, particularly if durability against compression is a requirement of the system. Recent studies show that the use of singular value decomposition in combination with other frequency domains for hiding data can further enhance an algorithm, with regard to image quality and security [7].

2.1 The Algorithm

Our approach adopts a combination of two effective transform methods, namely, DWT and SVD. DWT decomposes the image into four frequency bands: LL (low frequency), HL, LH (mid-frequency), and HH (high-frequency). The HH band is selected to embed the secret data as it holds only minor details, and its contribution is almost insignificant to the energy of the image, thus data embedding will not disturb the perceptual fidelity of the cover image. Furthermore, low frequency sub-bands (LL) can only be altered to a certain extent; otherwise it would have a serious impact on image quality [10] observed that the Human Visual System (HVS) fails to differentiate changes made to the HH band. This algorithm presents a procedure which will replace the singular values of the HH sub-band with the singular values of the secret image. The singular values of the HH band of 5 test images are presented in Table 1. Notice that the singular values are somewhere between 92 and 177. If the singular values of the chosen secret image lie within a similar range, then no significant degradation to the cover image will occur, due to the SV's of hidden image being similar to those of the HH band.

Table 1. Singular values of HH frequency band of different test images

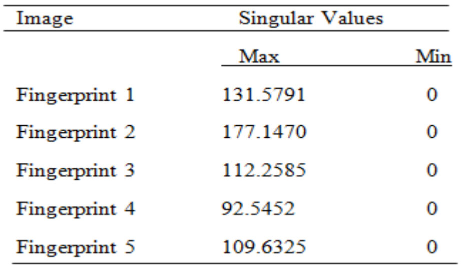


Image	Singular Values	
	Max	Min
Fingerprint 1	131.5791	0
Fingerprint 2	177.1470	0
Fingerprint 3	112.2585	0
Fingerprint 4	92.5452	0
Fingerprint 5	109.6325	0

All images used for the purposes of experimentation were taken from the Fingerprint Verification Competition (FVC2004) database [11] and the Yale Face Database B [12]. The Yale website contains many databases, however only the B database is authorized for research purposes. The use of other databases first, requires permission. Prior to embedding, Adobe Photoshop was used to alter all images to a specific size (512x512) and format (bitmap), the size of the facial images is also made identical to the size of the HH sub-band, where data embedding will take place. Preceeding data embedding, an important aspect concerning the feature extraction of fingerprint data must be considered. Features extracted from a fingerprint, namely minutiae, are used to determine a person's identity. It is imperative that the locations of these important regions are not altered during the embedding stage [13]. To ensure these regions are not affected during the embedding stage, fingerprint minutia are identified and extracted from images before, and again, after embedding [14].

2.2 Fingerprint Image Processing

Fingerprints from the FVC database [11] were used therefore, no acquisition step is implemented. Image Binarization is applied to the fingerprint image. This process transforms the 8-bit fingerprint image to 1-bit image. In general, an object pixel is given a value of "1" whereas a background pixel is given a value of "0." Subsequently, a binary image is generated by shading pixels, either black or white (i.e. black for 0, white for 1). Here, a locally adaptive binarization method is performed using Matlab "im2bw" function. The approach used here divides the image into (16x16) blocks and calculates the mean intensity value for each block. Then, each pixel value is changed to "1" if its intensity value is greater than the mean intensity value of the current block, to which the pixel belongs to. After the fingerprint image is converted to binary form, a thinning algorithm is applied to reduce the ridge thickness to one pixel wide. In order to preserve fingerprint minutia, it is important that the thinning operation be performed without any modification being made to the original ridge. For this purpose, MATLAB's built in morphological thinning function "bwmorph" is used. The "bwmorph" operation is based on the following two principles, ridge end points are not removed and connected ridges are preserved. The function is applied as follows: bwmorph(binaryImage,'thin',inf) takes a binary image as input, applies the thinning procedure which in turn, outputs a skeletal binary image consisting of only one pixel wide. Figure 1 presents a fingerprint image before and after thinning.

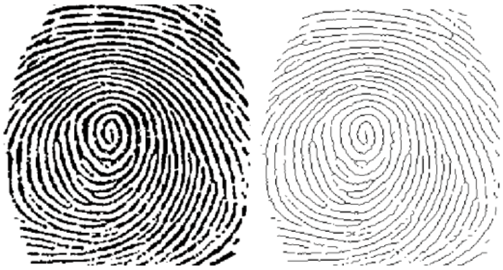
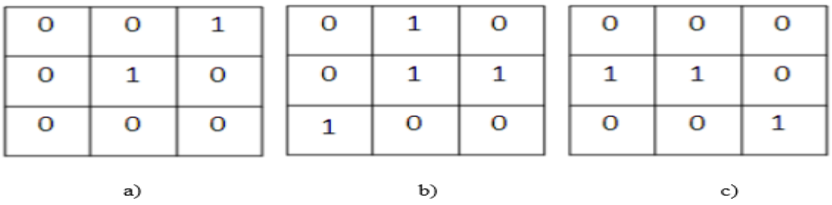


Figure 1. Before and after thinning

The aforementioned function uses an iterative, parallel thinning approach which scans over a (3x3) pixel window, checking the neighbourhood of a pixel based on a number of conditions [15]. Upon every scan of the fingerprint image, redundant pixels are marked down within each image window (3x3). After several scans, all marked pixels are removed thus providing a skeleton image.

Succeeding binarization and thinning, the process of extracting fingerprint features is relatively straightforward. A concept known as crossing numbers (CN), originally proposed by [16] is used. This is an important step in fingerprint recognition, as the bifurcation and terminations will be determined. The crossing number concept is carried out based on a 3x3 window, if the central pixel in the window is 1 and has only one-value neighbour, then the central pixel is an end-point (i.e. ridge ending/termination) presented in Figure 2(a). If the central pixel is 1 and has exactly 3 one-value neighbours, then it is a bifurcation as shown in Figure 2(b). Finally, if the central is 1 and has 2 one-value as neighbours, then it is a non-minutia point as illustrated in Figure 2(c).



0	0	1
0	1	0
0	0	0

a)

0	1	0
0	1	1
1	0	0

b)

0	0	0
1	1	0
0	0	1

c)

Figure 2. Indication of minutia points

The pre-processed fingerprint image contains many false minutiae, such as breaks, spurs, bridges etc. illustrated by circles in Figure 5. This can be due to insufficient amounts of ink, which cause false ridge breaks, or over-inking in which ridges can cross-connect. It has also been noticed that some of the pre-processing stages carried out have added to the problem of false minutia. Spurious minutiae can have a significant impact on fingerprint recognition. For instance, if fake minutia is regarded as genuine, system accuracy will be poor. Therefore, it is an essential requirement that false minutiae are eliminated. For this purpose, the Euclidean distance method is used [17]. The 3 step process to remove false minutia is: 1) If the distance between a termination (end-points) and a bifurcation is smaller than D, this minutiae is removed; 2) If the distance between two bifurcations is smaller than D, remove minutiae and 3) If the distance between two terminations is smaller than D, this minutia is also removed. Figure 3 presents fingerprint images before (a) and after (b) removal of false minutiae. Note: terminations are circled in red, bifurcations in green.

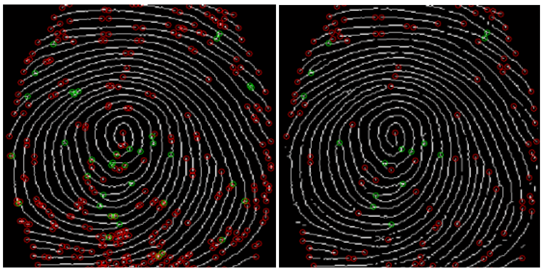


Figure 3. Fingerprint before (a) and after (b) removal of false minutiae

After the removal of spurious minutia, features of the fingerprint image can be eliminated further. For example if we consider Figure 3(a), note that a lot of minutiae are contained around the edges, this is known as background information, often generated when the ridges are out of the sensor. To eliminate this area, a region of interest (ROI) is recognised for each fingerprint. This procedure was carried out using Morphological ROI tools from MATLAB [18].

The two operations used in ROI extraction are "OPEN" and "CLOSE". The use of the 'OPEN' function will expand the images by a specified size and eliminate existing background noise such as, peaks. The "CLOSE" function is then used to shrink the fingerprint images and close up any tiny holes or gaps that may exist within the image. The bound region is determined by the subtracting the closed area of the image from the opened area. Then the left, right, upper and bottom blocks are discarded, leaving only the inner area of the image, known here as region of interest which is illustrated in Figure 4.

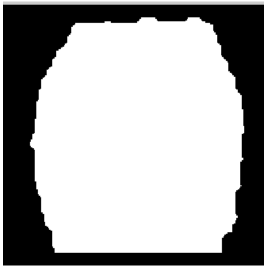


Figure 4. Region of Interest

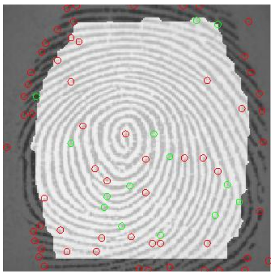


Figure 5. Fingerprint image after Region of Interest is applied

After the ROI is defined, all minutiae external to this region are suppressed, as the important minutia lies only within the inner section of the image. Figure 5 presents a fingerprint image showing external and internal minutia after ROI is applied. Finally, minutia contained in the inner area of the image is saved to a text file.

2.3 Securing fingerprints biometrics

The next step of the algorithm is to secure the fingerprint biometric with the use of steganography. For this purpose, another piece of biometric data (facial image) is used. It is believed that embedding one biometric within another can further enhance the security of the system, as two forms of authentication will then exist [19]. The fingerprint image will be referred to as cover image, and the face image as secret image. When the secret image is embedded into the cover image, this will be introduced as the stego image. Figure 6 shows the embedding (a) and extraction (b) of secret data in the transform domain using the SVD technique.

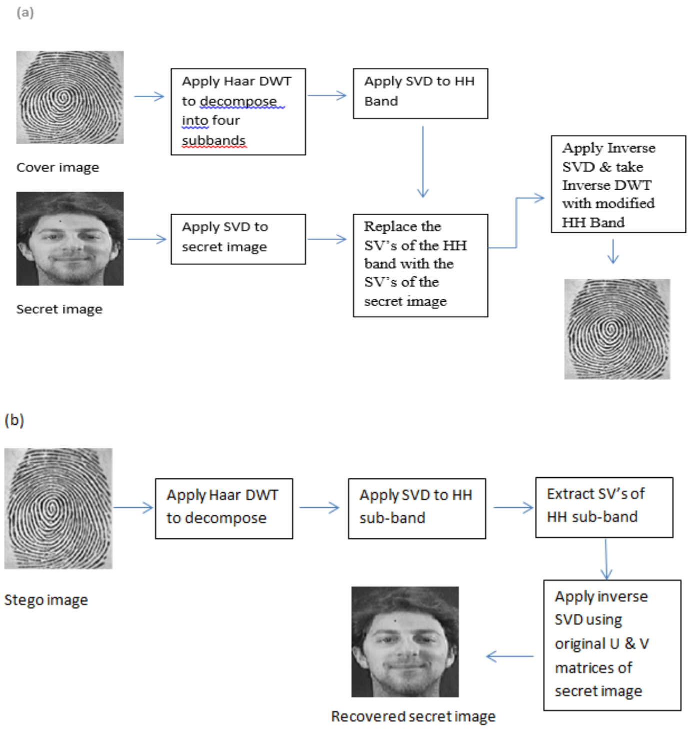

(a)
Cover image
Apply Haar DWT to decompose into four subbands
Apply SVD to HH Band
Secret image
Apply SVD to secret image
Replace the SV's of the HH band with the SV's of the secret image
Apply Inverse SVD & take Inverse DWT with modified HH Band
(b)
Stego image
Apply Haar DWT to decompose
Apply SVD to HH sub-band
Extract SV's of HH sub-band
Apply inverse SVD using original U & V matrices of secret image
Recovered secret image

Figure 6. Embedding (a) and Extraction (b) Algorithm

After the embedding, the secret image was extracted and clearly recognizable. Modifying only the singular values of an image allows for the data to be extracted without the need for the original cover image. This has benefits in regards to security as the original image does not need to be stored.

2.4 Image Attacks and Quality Measures

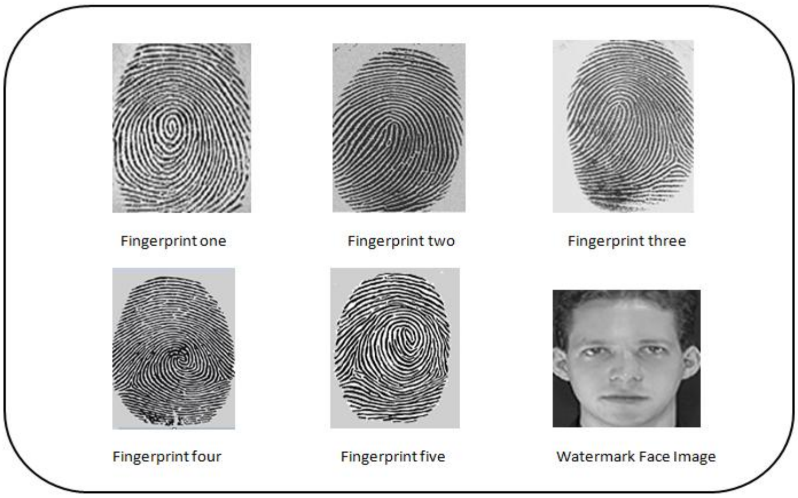
In order to prove the robustness of the data embedding technique proposed, a series of attacks have been carried out on the stego fingerprint images. It is common to compare two images using PSNR (peak signal to noise ratio) based on the MSE (mean-squared error). However, if data is specifically embedded within the image edges or textured areas, PSNR is then an inefficient method to compute the quality of an image [20]. In [21], a selection of methods have been proposed to overcome PSNR disadvantages. An objective formula often used for comparability purposes is the Normalized Cross-Correlation (NCC). This metric is used to measure deflections between the extracted facial image (after attacks) with respect to the original facial image (prior to attacks). If the NCC value is equal to 1, then the embedded data and the extracted data are same. Typically, if the NCC value is greater than 0.7500, it is accepted as a reasonable data extraction. All of the above are important steps in order to enhance fingerprint security. The most decisive one being that minutia must still be extractable from the fingerprints after the data embedding procedure, and image attacks have been carried out. Even though the facial data extracted from the fingerprint is clear, it would be considered a failure if minutia was severely altered during data embedding in such a way that user authenticity would be affected. For this reason, all stego fingerprints (after embedding and attacks) are put through the feature extraction process, and minutia extracted before and after the steganography process is compared. There is no standard number of minutiae required in order to make a positive identification. In some cases, the decision as to whether or not the fingerprints match is left solely to the examiner. However, each individual department may hold their own set of requirements in order to establish a positive identification. Ireland follows what is known as an 8-point rule, meaning that 8 minutia points are required for a valid identification. Many European countries require no less than 12 points of similarity [22]. The UK and Italy require 16, while Brazil and Argentina require not less than 30 Nonetheless, it is obvious that the more minutiae points exist, the more accurate the identification process will be.

3. Evaluation

The strengths and weaknesses of the proposed technique were investigated with regards to invisibility, robustness against various image processing attacks and possible detection using Steganalysis tools. Although, five test images were used for test purposes, this section will only discuss, and display detailed results based on one fingerprint image (fingerprint one). However, the results from the additional four fingerprint images will occasionally be referred to, and compared with the results of fingerprint one.

3.1 Image Database

To allow for a fair comparison regarding results, it is important that any steganographic software is tested on many different images. We used the FVC (Fingerprint Verification Competition) dataset which includes four disjoint fingerprint databases (DB1, DB2, DB3, and DB4). Five test images were used, each of size 512x512 pixels. They will be referred to as fingerprint one, two, three, four and five as illustrated in Figure 7. A facial image from the Yale Face Database B [12] will be embedded within each fingerprint image.



Fingerprint one

Fingerprint two

Fingerprint three

Fingerprint four

Fingerprint five

Watermark Face Image

Figure 7. Fingerprint images and watermark face image

3.2 Minutia Extraction

Before the embedding process, five test images were loaded into our minutia extraction GUI. As mentioned earlier, it is important that minutiae are not severely harmed whilst embedding the facial watermark. Table 2 summarises the number of minutiae extracted from each fingerprint image prior to embedding. The number of bifurcations and terminations are given for each individual image.

Table 2. Minutiae extracted from five fingerprint images before embedding

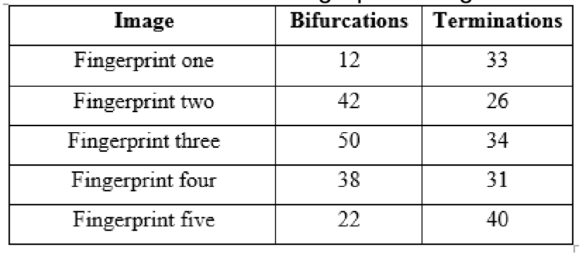
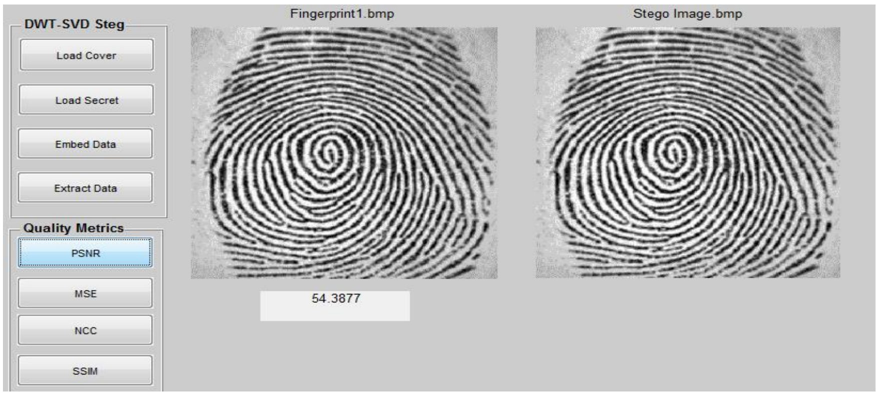


Image	Bifurcations	Terminations
Fingerprint one	12	33
Fingerprint two	42	26
Fingerprint three	50	34
Fingerprint four	38	31
Fingerprint five	22	40

Considering the extracted minutia, it is observed that the amount of bifurcations and terminations vary. Fingerprint one has only twelve bifurcation points whereas fingerprint three has fifty. This is because each fingerprint has its own unique pattern hence no two fingerprints can have identical minutiae.

3.3 Image Quality Analysis

After the embedding procedure, a visual examination of each image was completed in order to determine variations between the original image and the stego image. As shown in Figure 8 the original image is “Fingerprint1.bmp” and the stego image is “Stego Image.bmp”.



54.3877

Figure 8. The original “fingerprint” and “fingerprint” images after the hybrid steganographic technique is executed

A cohort of eight was used for testing. Each person was given one minute to study the two images. Any evidence or indication that data was hidden, such as the file names below each image were removed prior to viewing. After studying the images, each person was asked if any differences were noticeable between the two images and if so to point them out. Six out of the eight individuals thought that the two images were the same, whilst the other two persons were uncertain and believed that the two images were different. However, when both were asked to highlight the differences, they were unable to do so without hesitation. Succeeding the above subjective test, the PSNR and SSIM were then calculated. Both tests were computed by comparison between two images, the original image and the stego image. A PSNR value over 38 decibels means that there are no noticeable differences between the two images being compared. If the SSIM test outputs a value of 1, this means the two compared images are identical. Table 3 gives a summary of results of PSNR and SSIM value for images all containing the watermark.

Table 3. PSNR and SSIM results for images all containing the watermark

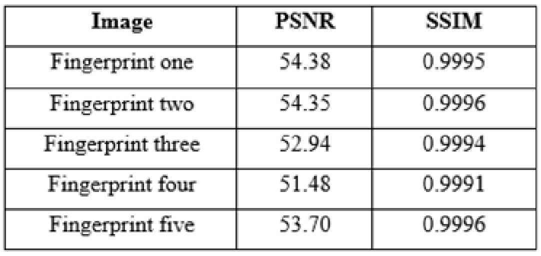


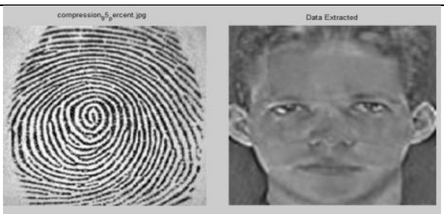
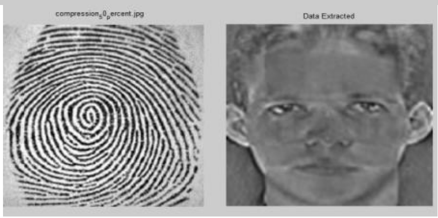
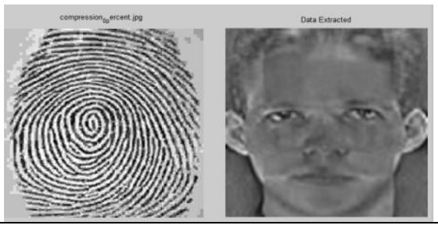
Image	PSNR	SSIM
Fingerprint one	54.38	0.9995
Fingerprint two	54.35	0.9996
Fingerprint three	52.94	0.9994
Fingerprint four	51.48	0.9991
Fingerprint five	53.70	0.9996

There are only slight differences in each PSNR value, for each image. For example, the highest PSNR value is 54.38 and the lowest is 51.48. The calculated PSNR for each image is high which therefore indicates that all images are of good quality after embedding. The SSIM values are all around 0.99, which indicates that there are no considerable differences between the original image and the stego image, even though data was embedded. The comparison of results, regardless of using different fingerprint images implies that the proposed hybrid technique should stay invisible regardless of the type of fingerprint image used.

3.4 Robustness Analysis

This section will evaluate the survival of the embedded watermark after attacks are carried out on the ‘fingerprint one’. The Normalized Cross Correlation (NCC) value is calculated to assess the distortion of the embedded watermark after each attack. JPEG Compression is a widely used technique for digital image compression therefore any steganography system should have some degree of durability toward compression algorithms. JPEG Compression is applied to the image ‘fingerprint one’ using different quality factors. For example, applying 5% of compression means that the image has a quality factor of 95%, meaning the image has a data loss of 5% and maintains 95% of its original detail. Table 4 gives a summary of results.

Table 4. Data survival after of the embedded watermark after JPEG compression is applied at various quality levels

Compression %	Normalized Cross Correlation (NCC)Value	Extracted Data After JPEG Compression
5	0.87	
50	0.49	
100	0.42	

The NCC value shows that the extracted watermark deteriorates after a higher level of compression is applied. However, the watermark is still clearly recognisable even after 100% of compression (0% JPEG quality factor). This test was also carried out on four other fingerprint images. The results are similar to the above. Based on these results, the proposed method is robust against all quality levels of JPEG compression.

JPEG2000 is another compression method that uses wavelets as opposed to DCT. After applying different levels of compression the NCC value only changes slightly. Data extracted after 10% of compression (90% JPEG 2000 quality factor) is almost identical to data extracted after 95% of applied compression (5% JPEG 2000 quality factor).

Two types of noise (Salt and Pepper and Gaussian noise) were added to the stego image. However, the NCC value confirms that the addition of noise has somewhat affected the watermark quality. Although the image quality is slightly flawed, the facial image is still identifiable. Results for the other fingerprint images were similar.

Rotating an image, even a tiny amount (0.1 degree), clockwise or anti-clockwise can be enough to disrupt the whole bit map thus may cause embedded data to be lost. The facial watermark survives rotation degrees between -1 and 1. The image quality is partially distorted however it is still very distinguishable after all attacks. Therefore it can be concluded that the proposed method is resistant to above rotation attacks.

Image cropping is a lossy procedure often used in real life. Here, three different sizes of cropping are applied to the stego image, respectively using MATLAB's 'imcrop' function. This function crops the fingerprint image by the size and position of the rectangle specified (i.e. rectangle is a four-element position vector [xmin ymin width height]. The results show that the proposed algorithm is resistant against some cropping attacks.

A common manipulation in digital images is median filtering. The median filter is a non-linear spatial filter which is often used to eliminate noise spikes from an image. Here the facial features of the watermark are still clearly recognizable after the above filtering attacks has been applied. Therefore we can say that the proposed steganography algorithm is robust against median filtering.

3.5 Minutiae Analysis

It is important that the data embedding process does not seriously alter the minutia points in the fingerprint image. Table 5 shows results of fingerprint minutiae extracted based on the five fingerprint images, pre and post data embedding. Bifurcation points is denoted as B and termination points as T.

Table 5. Minutia extraction results for pre and post data embedding

Image Name	Original Image		Stego Image	
	B	**T**	**B**	**T**
Fingerprint one	12	33	10	32
Fingerprint two	42	26	38	26
Fingerprint three	50	34	43	32
Fingerprint four	38	31	38	31
Fingerprint five	22	40	21	40

Note: Bifurcation points is denoted as B and termination points as T

Based on comparison of the minutiae results, before and after the data embedding, it can be concluded that some minutiae points have been affected slightly. For example, 'fingerprint one' lost two bifurcation points and one termination point, minutiae in the remaining images have also been somewhat modified, fingerprint four being the exception, with no minutia loss. No standard number of minutia is required in order to make a positive identification. However, the number of minutia points required vary from country to country, with Brazil and Argentina requiring the highest amount (minimum of 30 points). Based on this knowledge, it is reasonable to assume that the proposed data embedding algorithm did not corrupt the fingerprint minutiae to an extent that it would interfere with the identification process.

In order to fully test the durability of minutiae, the extraction process is also carried out on stego images that have been attacked by JPEG and JPEG2000 compression, noise addition, filtering, and geometric attacks. Although, five test images have been used for experimentation, only results based on 'fingerprint one' will be presented here. The attacked images will be named based on the attack applied to them. So for example, an image attacked with JPEG compression will be denoted as 'JPEG5%, 5% signifying the image quality factor. Or, an image attacked with salt and pepper noise will be listed as 'salt & pepper20%, 20% meaning 20% of image pixels were modified. Similar to above, bifurcation points are denoted as B and termination points as T. Table 6 shows results for minutia extracted from attacked images, minutia extracted from original image (i.e. fingerprint one) and minutia extracted after watermark is embedded into the original image (i.e. stego image).

The results show that the fingerprint minutia is robust and can tolerate various level of JPEG and JPEG2000 compression. After 10% compression (quality factor of 90%) results show no change in minutiae. After applying a high compression rate (95%- quality factor 5%) minutia loss is significant however, not an adequate amount of fingerprint minutiae has been disturbed in the sense that it would prevent an accurate identification. As can be seen in Table 6, the noise attacked images has altered minutia significantly. Both Salt & pepper and Gaussian noise addition has resulted in additional bifurcation points being added to the image. This spurious minutia may cause problems such as, extraction of false minutiae. Filtering attacks have also disturbed minutia features. The histogram attacked image shows a lot of additional minutiae. However, no addition of minutiae exists in Gaussian and median attacked images. So, it is reasonable to say that the two out of the three filtering attacks (Gaussian & median) would not prevent an accurate identification process from taking place. Geometric attacks have considerably modified minutia points. However, extracting valid minutia from the resized image (200x200) may still be feasible based on the fact that only one termination point has been added. This cannot be said for the rotated image, as the amount of termination points has almost doubled. Lastly, the cropped image has lost all existing minutiae. This is no surprise, and is most likely due to the region of interest being excluded as a result of cropping. These results demonstrate that fingerprint minutia is resistant against the JPEG and JPEG2000 compression and also proves robust against two of the tested filtering attacks.

Table 6. Fingerprint one minutiae survival results after attacks

Image Name	B	T	B	T	B	T
	Extracted minutia from attacked images		Extracted minutia from original image (fingerprint one)		Extracted minutia from stego image	
JPEG5%	7	30	12	33	10	32
JPEG50%	9	30	12	33	10	32
JPEG90%	10	32	12	33	10	32
JPEG2000	9	32	12	33	10	32
Salt & pepper20%	20	31	12	33	10	32
Gaussian20%	13	33	12	33	10	32
Histogram	37	26	12	33	10	32
Median3x3	7	25	12	33	10	32
Gaussian blur	6	32	12	33	10	32
Resize200x200	6	33	12	33	10	32
Rotation by 50	8	37	12	33	10	32
Crop300x300	0	0	12	33	10	32

4. Conclusion

The aim was to develop a watermarking algorithm, inspired by steganography techniques, for digital images, to protect fingerprint biometric data in biometric security. As DWT and SVD transforms are used simultaneously, the fundamental advantages of both the transforms are obtained. General image processing techniques do not alter singular values of digital images thus the use of SVD makes this method more robust than the use of DWT alone. Noise attacks as well as image processing operations can be sustained, hence robustness is achieved. In this work, a hybrid data hiding algorithm which combines the DWT and SVD transforms has been used. After decomposing the original fingerprint image into four sub bands (LL, HL, LH and HH), SVD is applied to the HH band and diagonal singular value coefficients are modified with the singular value of the watermark itself. Subsequently, HH band coefficients are reconstructed with the modified singular values and lastly, the inverse DWT is applied to obtain the stego image. Our results show that the proposed scheme is undetectable using visibility checks. Moreover, the steganalysis tools used also failed to detect it. This demonstrates that the hybrid algorithm is undetected. Results clearly show the proposed techniques robustness to a considerable number of attacks, such as image processing attacks and many levels of geometric attacks, up to the point where any commercial value of the tested images are lost. The proposed method also proved durable to various levels of JPEG/JPEG2000 compression attacks, and according to research, the need to compress biometric data is essential in order to limit storage space. However, after a resizing attack of 90% was applied the watermark deteriorated badly, and as a result did not survive this attack. On the aspect of preserving fingerprint features after data embedding, the fingerprint minutiae showed good resilience against the proposed embedding process and some attacks. Thus, fingerprint images were watermarked with little or no change to the features associated with them. Our system offers a good combination of imperceptibility and robustness for digital fingerprint images watermarked with a facial image using a combined method of the SVD and DWT transforms. In addition, the original image is not required to extract the hidden data, which further enhances data security.

References

[1] Yogarajah, Condell, J Curran, K Cheddad A, Mc Kevitt. A Dynamic Threshold Aproach for Skin Segmentation in Color Images International Journal of Biometrics. 2012; 4(1): 38-55. ISSN: 1755-8301, DOI: 10.1504/IJBM.2012.044291

[2] Nandakumar K, Jain AK. Biometric Template protection Schemesp Bridging the performance Ga: Between Theory and practice, *IEEE Signal processing Magazine*. 2015; 32(5): 88-100.

[3] Galbally, J Fierrez, J Alonso–Fernandez, F Martinez–Diaz, M. Evaluation of Direct Attacks to Fingerprint Verification Systems.*Telecommunication Systems (Springer)*. 2011; 4-3(3-4): 243–254.

[4] Georghiades, A.S. *The Yale Face Database B.* 2011. http://vision.ucsd.edu/~iskwak/ExtYaleDatabase/Yale%20Face%20Database.htm.

[5] Jain, A Uludag U. Hiding biometric data, IEEE Trans. Pattern Analysis and Machine Intelligence. 2003; 25: 1494-1498.

[6] Cox I Miller, M Bloom, J Fridrich, J Kalker T. *Digital Watermarking and Steganography*. 2nd ed. USA: Kaufmann. 2008: 1-2.

[7] Saha, B Sharma S. Steganographic Techniques of Data Hiding using Digital Images. *Defence Science Journal*. 2012; 62(1): 11-18.

[8] Subhedar, M Mankar VH. High Capacity Image Steganography based on Discrete Wavelet Transform and Singular Value Decomposition. International Conference on Information and Communication Technology for Competitive Strategies. 2015,

[9] Lusson F Bailey, K Leeney, M Curran K. A Novel Aproach to Digital Watermarking, Exploiting Colour Spaces. *Signal processing*. 2012; 93(5): 1268-1294.

[10] Dhandapani, S Ammasai K. Robust Digital Image Watermarking for Color Images. *European Journal of Scientific Research*. 2012; 76(1): 117-126.

[11] Gupta AK, Raval MS. A robust and secure watermarking scheme based on singular values replacement. *Indian Academy of Sciences*. 2012; 37(4): 425-440.

[12] Maltoni, D Maio, D Jain A.K Prabhakar S. Handbook of Fingerprint Recognition. 2nd ed. London: Spinger. 2009: 58-60.

[13] Li, Y Georghiade C, Huang G. Sequence estimation for space-time coded systems. *IEEE Trans. Commun*. 2001; 49(6): 948-951.

[14] Bazen A, Gerez S. *Extraction of singular points from directional fields of fingerprints. In Mobile Communications in perspective.* Proc. CTIT Worksho: on Mobile Communications. University of Twente, Enschede, The Netherlands. 2001: 41–44

[15] Kussener F. 2007. *Fingerprint Aplication.* http://bit.ly/2jxIPW7

[16] Mahdi, AM Hanoon A. Fingerprint Recognition. *Journal of Engineering and Development*. *IET*. 2011; 2(1): 21-27.

[17] Arcelli, C Baja G. A width independent fast thinning algorithm. IEEE Transactions on Pattern Analysis and Machine Intelligence. 1985; 4(7): 463-474.

[18] Deza, M Deza E. *Encyclopedia of Distances*. Springer. 2009: 94-96.

[19] Matlab. *Image Processing Toolbox.* 2015. Available: http://uk.mathworks.com/hel:/images/index.html.

[20] O'Gorman L. Fingerprint Verification. In: Jain, A Bolle, R Pankanti, S Biometrics: Personal Identification in Networked Society. USA: Springer. 2006: 44-62.

[21] Wang, Z Bovik, AC Sheikh, HR Simoncelli EP. Image Quality Assessment: From Error Visibility to Structural Similarity. *IEEE Transactions on Image Processing*. 2004; 13(4): 46-52.

[22] Cheddad, A Condell, J Curran, K McDevitt P. Digital Image Steganography: Survey and Analysis of Current Methods. *Signal Processing*. 2010; 90(3).