STEGANOGRAPHY OF FINGERPRINT IMAGES BY USING DISCRETE WAVELET TRANSFORM

Farinaz Dehestani Kolagar, Seyed Mohammad Jalal Rastegar Fatemi
Department of Electrical Engineering, Saveh Branch, Islamic Azad University, Saveh, Iran.
j_rastegar@iau-saveh.ac.ir, farinazdehestani_1368@yahoo.com

ABSTRACT
Wavelets are certain functions that are comparable in terms of shape to Cos and Sin functions based on Fourier analysis. For two-dimensional images, applying the discrete wavelet transform (DWT) is corresponding to the image processing in any dimension by two-dimensional filters. The input image divide by filter into four non-overlapping sub-bands with multi-band HH, HL, LH and LL resolutions. Unacceptable results of steganography made by the wavelet transform caused to use the RDWT due to the low sampling, the changed form of image steganography and the undesired extraction of hidden image in the simulation stages. We will apply SVD to the LL sub-bands after applying RDWT to both front part and watermark image of the picture. Then single values of the front image correcte by using single values of watermark image. Resistance against common attacks is the proposed technique’s advantage. Analysis and empirical results show the better performance of the proposed method in comparison with other methods.

KEYWORDS: Wavelet, Rdwt, image watermarking, Svd

INTRODUCTION
Human fingerprint is a trace of finger tip’s grooves. Fingerprint can be used to identify individuals since no two people have a same fingerprint. Steganography always has been of human interest therefore hiding information by invisible inks, secret codes, secret messages and … have a long history. Herodotus, the Greek historian, for the first time has described two examples of steganography in a book called "histories" around the year 440 BC. The first case has been in Susa, when the Greek governor, had been imprisoned by Darius the Persian sovereign. He must confidentially send a message to his step brother in Miletus, thus shaved his slave's head hair and made the message as a tattoo on his head. When the slave's hair had grown enough to forward him to Miletus in order to shave his hair to get the intended message. The second case was reported at the time of Cyrus, king of Persia, that Demaratus was a Greek in Persia court that he sent a secret message to Greece governor to inform him of the Cyrus attack. At first he removed the wax on a plat and wrote his message on the wooden plat and then hid the message again with wax so that the plat was exactly similar to a plat with no written message on it. German priest, Trithmus was one of the pioneers of steganography and wrote a book titled “Steganographia” which was not published during his lifetime. In the domain of transform in steganography, wavelet transform domain is one of the highly regarded domains. Wavelet transform was proposed by the Haar in 1908 AD for the first time and after that some researchers change it forms until it has become its present form. One of the major reasons of wavelet transform using is its similarity to the human visual system. Human retinal divide images into several frequency channels which the bandwidth of each channel is almost one octave. Biometric technology is now essential for the identity detection and authentication. Currently the need for security in electronic trades necessitates the using of reliable factors such as the structure of the fingerprint. Steganography of fingerprint is used in applications such as originality protection of fingerprint images stored in the database against intentional and unintentional attacks, fraud detection in fingerprint images and guarantee the secure transmission of fingerprint images. In this research we are looking for using of the wavelet transform for steganography of fingerprint image.

Image steganography area increases dramatically over the past decade. This advancement that is mainly proportional to the data increasation, include the increasing amount of visual information easily transmitted through digital devices or browse by them. Image steganography is widely used as an effective way to study the appearance integrity and digital data originality. Most of complex ideas in this area, initially proposed by barney and et al (Barni & Bartolini, 2001). Their idea were inspired by the behavior of HVS in determining the value of tangible changes in the discrete
wavelet transform (DWT) amplitude for lossy image compression. In recent years, many researchers have focused on the fingerprint image steganography research. Undoubtedly one of most important factors that has made this method superior in comparison with other biometric methods is abilities of this system in eliminating existent shortcomings of the old system (Uludag, 2006). Without a high level of security, no information or data is not safe against hackers attack. But for protection of information resources and data, should gradually moved towards more important factors and modern methods. Among all techniques of identification, fingerprinting is the oldest method that successfully applied in various fields therefore it caused database information protection of security systems have a high importance. In fact, these systems enhance the security in a manner that an attacker from outside of the security system wouldn’t be able to manipulate data in a person's fingerprint and can not access to the fingerprint in the system, as long as watermarked image has not been extracted. In such safety systems extracted image is used for identification as a document and since they have a high security are used with a high confidence in the database. Various techniques of steganography are presented to protect the fingerprint information that leads to interesting results in this respect (Cao & et al, 2010).

So far numerous works has been done in the field of image steganography such as steganography by transferring image to another area and inserting watermark image in it. To mention areas that are used for this purpose, can mention frequency domain transfers that are generally used for digital images steganography algorithms and including following transfers: Discrete cosine transformation (DCT), Discrete Fourier transformation (DFT) and discrete wavelet transformation (DWT). Among works done by a discrete Fourier transform is the embedding a random signal in the amplitude of middle bands Fourier transform coefficients (Craver, 1998). Also other works has been done by using the discrete Fourier transform (Chi-Man Pun, 2006). Some works has been performed in the field of steganography by discrete cosine transform (Dongyang Teng, 2010). In these methods the discrete cosine transform apply on the image and steganography apply after transferring image to the desired area and the original image rebuilt by an inverse transformation. Some works has been done by wavelet transform that in these methods image wavelet transform obtained and embedded the desired information in it after obtaining wavelet coefficients (Pournader &lagziyan, 2002).

Among these methods, DWT is more considerable for its multiple resolution property and perfect image localization that is similar to the theoretical models of the human visual system. In recent years, steganographymethods with the wavelet transform has used for important steganography projects such as fingerprint steganography and image of the iris (Zebbiche, 2014 & Majumder, 2013).

Singular Value Dimension

Steganography can be performed in transformation amplitude or spatial domain. Spatial domain methods are less complex but don’t have the scope of transformation resistance against various attacks [5]. In order to better understanding of available methods we express the background of implemented methods at the beginning and then we present our proposed method. One of the most common technique in the transformation amplitude steganography is the correction of obtained coefficients from single value decomposition (SVD) of cover image. Based on steganography algorithm, SVD was first proposed by Liu and et al. In this algorithm, authors after applying singular value decomposition to the cover image, modify these coefficients by adding the watermark. They apply SVD transform to the outcome matrix again in order to find corrected singular values. In a similar work, embedded singular values of watermarking in total singular values of host image. The most important defect of based on SVD algorithm is the watermark image quality degradation. In addition, the extracted watermark image has sufficient resistance against common attacks in based on SVD algorithms. Researchers usually compound SVD with other algorithms such as DCT and DWT. In the (Vosoghiniya, 1385), authors combine DWT with SVD technique. In that paper after decomposition of the host image into four sub-bands, SVD is applied to each sub-band and embedded watermark single values in sub-bands. In the (Hashemi, 1385), DWT and SVD technique are combined to hidewatermark single values in the image high band (HH) frequency. When DWT combine with SVD technique, steganography algorithm operates beyond the conventional DWT algorithm according on resistance against Gaussian noise, compression and cropping attacks (Fabien, 1999) and cutting (Fabien, 1999). Despite the good performance of DWT techniques in the steganography, this technique suffers of defects that will discuss in further discussion. To overcome the steganography defects based on DWT, a solution is using of redundant discrete wavelet transform (RDWT). For this purpose firstly we’ll describe wavelet then present explanation for redundant discrete wavelet transform.
Redundant Discrete Wavelet Transform

One of the common available methods for steganography is DWT but the main defect of this method is that moving is not stable due to the low sampling of these bands. Even for a small movement in the input image, this defect caused a major change in the wavelet coefficients. The heterogeneity of DWT displacement causes imprecise extraction of cover images and steganography (Patrick and Nick, 1999), while asteganography, it is required for cognition the exact location where steganography data are embedded. So for resolve this problem, researchers suggest using the redundant discrete wavelet transform. To explain RWT, one 1D DWT and RDWT with its inverse are shown in the figure (Gutub, 2009), which [ln] and [f[n] are input and rebuilt signals. The [h[k]] and the [g[k]] are low-pass and high-pass filters and [h[k]] and [g[k]] are combination filters of relevant high-pass and low-pass filter. [cj] and [dj] are output coefficients of high band and low band at level j. Analysis and composition of RDWT in (Gutub, 2009). are as follows:

Analysis:
\[ c_j[k] = (c_{j+1}[k] * h[k]) \]
\[ d_j[k] = (c_{j+1}[k] * g[k]) \]

Synthesis:
\[ c_{j+1}[k] = 0.5(c_j[k] * h[k] + d_j[k] * g[k]) \]

Where * denotes the convolution.

RDWT removes up and down sampling of coefficients at each filter bank iteration. Providing redundant of input sequence obtain by using of explant removal in the RDWT analysis. The signal processing based on RDWT is more resistant than DWT method once form extention increases the resistance due to increasing noise.

The proposal method:
Steganography based on a combination of RDWT and SVD is the proposal method.

Embedding watermark:
The proposal watermark embedding algorithm is shown in Fig1.

![Figure 1: Block diagram of proposal watermark embedding algorithm](image)

Stages of watermark embedding algorithm is as follows:

1. Apply RDWT to the cover image in order to decompose it into sub-bands LL, HL, LH, HH.
2. Apply SVD to the low frequency subband LL of the cover image:
   \[ I^l = U^l S^l V^l \]
3. Apply RDWT to the watermark image.
4. Apply SVD to the low frequency subband of the watermark image:
   \[ W = U^w S^w V^w \]
5. Modify cover image single values with watermark image single values.
   \[ S^{vl} = S^l + a S^w \]
   Where \( a \) is the scale parameter and \( a S^w \) and \( S^l \) are diagonal matrix of single values of cover and watermark image.
6. Apply inverse SVD to the transformed cover image modified by single values
   \[ l^{vl} = U^{vl} S^{vl} V^{vl} \]
7. Apply inverse RDWT by using low frequency bands modified coefficients to get the image with watermark.

Watermark extraction:
The Proposal Watermark extraction algorithm is shown in Figure 4-9.
Figure 2: Block diagram of proposal watermark extraction algorithm

1. Decompose image with watermark by using RWDT into four sub-bands: HH, HL, LH, LL.
2. Apply SVD to the low frequency sub-band LL:
   \[ I^{*1} = U^{*1} S^{*1} V^{*1} \]
3. Extract single values from the low frequency sub-band of cover and watermarked images:
   \[ S^w = (S^w - S^1) / \alpha \]
   Where and include single values of cover image
4. Apply inverse SVD in order to get low frequency coefficients of transformed watermarked image.
5. Apply inverse RDWT by using coefficients of low frequency sub-band in order to get watermark image.

To compare images and watermarking implement, two images lena and cat is used as the main image and two fingerprints images 1 and 2 is used as the watermarked image.

Figure 3: Images used to watermarking

To better understanding of the wavelet application, in this section we will apply wavelet algorithm on above images. Multidimensional decomposition of image capability is one of so good features of DWT. This feature gives you the ability to achieve well distinguish in different frequencies by using multi-stage wavelet decomposition and searching and watermarking at different wavelet coefficients. For this purpose in the early stages of simulation, we decomposed watermark image and cover image by using wavelet transform and then we collect watermark image and cover image.
by using 0.1 LL decomposition coefficient and Finally, we extract the watermarking image by wavelet inverse transform.

Figure 4: Illustration of the main image of cat and the watermark image

Figure 5: Illustration of the original fingerprint image and extracted image after watermarking

We observe that if the watermark image even by a factor of 0.1 in LL decomposition add to wavelet coefficients of original image, still the effect of watermark image remains on the cover image that is not acceptable in no way. The effect of application this algorithm on the image of Lena below to see is shown in the following figure:

Figure 6: The original Lena image and the watermarked image

Figure 7: Image extracted after watermarking

Since transformation of wavelet is one of the most common application of wavelets in steganography of images, at the beginning of simulation, various steps of the work were tested using DWT algorithm and it was found out that it doesn’t meet project requirements. Therefore, authors tested many methods and finally, combining RDWT and SVD yielded the suitable results. A sample of steganography in brands is shown in Lena image. Size of original image is
negligible compared to that of our simulation. Volume of the fingerprints applied by author in simulations is 512×512; while in latencies we used for protecting copyright has a low volume about 8×8 pixels. The next tip which is of great importance is the method of right extraction and similarity of extracted images to original one and this issue is of lower importance compared to copyright. However, in issues for which we send images such as fingerprint image, any blur and lack of clarity, will corrupt the overall performance of the project. In what follows, a sample of simulation on Lena image using DCT is represented.

Fig. 8: original image of Lena and watermarked image

Fig. 9: 20×20 pixels image extracted from Lena image

Duration of steganography in this image is 1.0296s and 0.4560s for image restoration. With respect to operation time, this is a good time, however, if we desire to do so for a movie of the same size, this time will be added up with times allocated for reading, writing and other operations. Essentially, steganography in movies is an issue which attempts to provide available algorithms in more advanced stages.

Fig. 10: image of cat and steganography image

Fig. 11: 50×20 pixels extracted image of cat

As can be seen in images, in lower sizes, majority of algorithms provide the suitable results; while the same algorithm will be repeated for no. 1 fingerprint image and it will be seen that 512×512 pixels image cannot have a good output from original image. To solve the problem, we can hide the fingerprint by changing its size so that no considerable change in the original image can be observed. Results are represented below.
Fig. 12: steganography performed on image in 1.0452s
Similarity of Lena image is acceptable to some extent. However, results of no. 1 image extraction is not convincing at all. This prompted us to consolidate our researches on similarity of watermarked image and original one so that we can be able to extract fingerprint image with maximum quality.

Fig. 13: 50x50 pixels image extracted from Lena image
For next test, we implement the algorithm on the cat image and it is observed that our results are repeatable.

Fig. 14: steganography performed in 0.9828s

Fig. 15: image extracted from cat image
In preliminary tests, we performed simulations on LBS algorithm. In what follows, we study the results of LSB algorithm and in next section, we illustrate our implemented algorithm using two fingerprints and provide the results.

Fig. 16: watermarked image of Lena by LSB algorithm and extracted fingerprint
As expected, LSB algorithm performs fingerprint extraction with a better resolution and Lena image is very similar to original one. However, due to unsuitable structure of the algorithm which performs the steganography in lowest level of the structure, this type of algorithm is not resistant against any attack. In next image which is tested by LSB, resolution results are repeated and extracted algorithm is exactly the same as original one.

![Fig. 17: watermarked image of Lena using LSB algorithm and extracted fingerprint](image1)

**CONCLUSION**

In steganography, two factors are of considerable importance. The first one is the volume of mark and image which is hidden from original one; that is, if the volume is lower, ability for steganography is higher due to availability of key and accordingly, the ability of others to reveal it will be lowered significantly. Our proposed method is based on the combination of RDWT and SVD methods. For this purpose, we represent the results of algorithm implementation on above images.

![Fig. 18: watermarked image of cat using SVD-RDWT algorithm](image2)

It is observed that steganography image is very similar to original one and has no distortion. Now, using inverse transformation, we extract the steganography image.

![Fig. 19: image of extracted fingerprint using SVD-RDWT algorithm](image3)

It can be easily seen that above algorithm is better able to perform steganography compared to DWT, LSB and DCT. Moreover, size of steganography image has no significant contribution to above algorithm and the value of correlation factor of the noiseless system is 0.9998 which is a satisfactory value. To further test the results, we implemented the results on Lena image. Results are shown below and to better observation, original image is represented as well.
Now, by means of inverse transformation, we extract the steganography image from Lena image.

Table 1: computation of PSNR using our proposed algorithm

<table>
<thead>
<tr>
<th>Noise Type</th>
<th>CC</th>
<th>PSNR</th>
</tr>
</thead>
<tbody>
<tr>
<td>GUASSIAN NOISE (VAR 0.001)</td>
<td>0.9941</td>
<td>29.36</td>
</tr>
<tr>
<td>SALT &amp; PAPPER (DENSITY 0.005)</td>
<td>.9976</td>
<td>30.62</td>
</tr>
<tr>
<td>ROTATE(50 DEGREE)</td>
<td>.8530</td>
<td>8.62</td>
</tr>
</tbody>
</table>

Similar attacks using DCT algorithm yields the following results.

Table 2: computation of PSNR using DCT method

<table>
<thead>
<tr>
<th>Noise Type</th>
<th>CC</th>
<th>PSNR</th>
</tr>
</thead>
<tbody>
<tr>
<td>GUASSIAN NOISE (VAR 0.001)</td>
<td>0.9532</td>
<td>25.14</td>
</tr>
<tr>
<td>SALT &amp; PAPPER (DENSITY 0.005)</td>
<td>.9053</td>
<td>24.12</td>
</tr>
<tr>
<td>ROTATE(50 DEGREE)</td>
<td>.652</td>
<td>6.7</td>
</tr>
</tbody>
</table>

Our proposed method provides the plan of steganography based on transformation of F discrete wavelet and decomposition of single value. After applying RDWT on fore and background, we apply the SVD to LL sub bands. Then, single values of the foreground will be modified using single values of the background image. Benefit of proposed method is its resistance against joint attacks. Experimental analysis and results reveal the better implementation of the proposed method over other methods.

REFERENCES


