Computer and Information Science; Vol. 8, No. 4; 2015
ISSN 1913-8989 E-ISSN 1913-8997
Published by Canadian Center of Science and Education

A Comprehensive Approach to Image Watermarking, Encryption and Steganography

Sabarish Sridhar[1]

[1] Department of Electronics and Communications, India

Correspondence: Sabarish Sridhar, Department of Electronics and Communications, MSRIT, Bangalore, India. E-mail: sabarishvs111@gmail.com

Received: August 18, 2015 Accepted: September 22, 2015 Online Published: November 6, 2015

doi:10.5539/cis.v8n4p32 URL: http://dx.doi.org/10.5539/cis.v8n4p32

Abstract

Steganography, water marking and encryption are widely used in image processing and communication. A general practice is to use them independently or in combination of two - for e.g. data hiding with encryption or steganography alone. This paper aims to combine the features of watermarking, image encryption as well as image steganography to provide reliable and secure data transmission .The basics of data hiding and encryption are explained. The first step involves inserting the required watermark on the image at the optimum bit plane. The second step is to use an RSA hash to actually encrypt the image. The final step involves obtaining a cover image and hiding the encrypted image within this cover image. A set of metrics will be used for evaluation of the effectiveness of the digital water marking. The list includes Mean Squared Error, Peak Signal to Noise Ratio and Feature Similarity.

Keywords: digital water marking, steganography, encryption

1. Introduction

Digital watermarking is similar to a stamp which is applied on images, videos, audio, programs, documents etc to prove the ownership. It is similar to the traditional watermark and is detectable only under certain conditions. Most of these digital watermarks are made invisible to the human eye but can be detected by the software. The digital watermarks have to be very robust. Illegal parties will try to remove the watermarks. Hence it is very important that the digital watermarks should be made robust. Watermark should remain unchanged even when it undergoes manipulation, copying, recording, compression, decompression, encryption, decryption, distribution etc. One prerequisite is that the watermark should not affect the original content in anyway.

Steganography aims to transmit secret messages through some unrelated content. The intended message is hidden inside the cover page. The latter has to be discarded by the receiver. The above two methods steganography and digital watermarking hide data. It is essential to understand at this point the difference between digital watermarking and steganography. The main aim of digital watermarking is to protect intellectual property rights and authentication of the content which is being transmitted or distributed. In digital watermarking, the watermark is always related to the content and both the content and the watermark are essential to the receiver. On the other hand, in steganography, there is no relation between the innocent looking content and the embedded secret message. The content is of no use to the receiver. The receiver has to extract the embedded secret message. Both steganography and watermarking hide data. This is different from the traditional concept of encryption where either the entire content is encrypted or an encrypted signature is added to the content. While the former restricts the free flow of the communication and also alerts hackers to the presence of encrypted data, the latter is susceptible to easy detection and removal of the encrypted signature.

In this paper we combine steganography, watermarking and image encryption. The required watermark is first inserted followed by encryption of the watermarked image. The final step is to hide this encrypted watermarked image within a cover image. The steps described in section Proposed Method Overview decreases the chances of any illegal use of the image, keeping in mind data integrity at the receiver side.

2. Previous Works

In 2001, Yusuk Lim, Changsheng Xu and David Dagan Feng, proposed a web based authentication system which has a watermark embedding system and an authentication system (Lim, Xu, & Feng, 2001). The user can

generate a watermark and embed it in the image. The watermarked image is transmitted. And the receiver uses the authentication system to receive the image. In 2003 MinWu and Bede Liu, suggested a new method to embed data in binary images. They used the concept of embedding a large amount of data after shuffling of pixels. This method was proposed to make the capability of embedding uniform throughout the image (Wu & Liu). In 2004 M.Dobsicek proposed a method where the content is encrypted with one key and can be decrypted with several other keys (Dobsicek). In 2005 Rehab H. Alwan, Fadhil J. Kadhim, and Ahmad T. Al Taani, proposed a method which used edge detection followed by LSB manipulation and ASCII encoding. Sobel filtering was used for edge detection (Rehab H, Fadhil J, & Ahmad T). Six bits of MSB were retained with the original image content whereas the rest were used for watermarking.

In 2007, Nameer N. EL Emam proposed a type of LSB insertion steganographic method which made it difficult for unauthorised steganography analysis tools to extract the data (Emam, 2007). In 2008 Prof S.K. Bandyopadhyay, Debnath Bhattacharyya, Swarnendu Mukherjee, Debashis Ganguly and Poulami Das have proposed a technique to hide huge amount of data. Here the data was first encoded and then hidden behind a cover image (SK, Debnath, Swarnendu, Debashis, & Poulami, 2008). In 2013, Youssra Lakrissi, Mohammed Erritali and Mohammed Fakir combined watermarking and encryption. The encryption was done using a secret key which in turn was encrypted an asymmetric algorithm. The encrypted image was then watermarked before distribution (Youssra & Mohammed, 2013).

3. Proposed Method Overview

The proposed method aims to combine the features of watermarking, image encryption as well as image steganography to provide reliable and secure data transmission. The first step involves inserting the required watermark on the image at the optimum bit plane. The second step is to use an RSA hash to encrypt the watermarked image. The final step involves obtaining a cover image and hiding the encrypted watermarked image within this cover image.

4. Image Quality Assessment

The visual quality of a digital image is subjective. The concept of better image quality varies from person to person. Hence it is difficult to say that one type of image processing is better than the other. This makes it necessary to establish quantitative/empirical measures to compare the effects of image content before and after watermarking, before transmission and after reception and before/after encryption. These metrics not only include conventional quality metrics like Peak SNR and Mean Squared Error, but it also includes Human Visual System (HVS) based quality metrics.

Over the last years many metrics have been proposed for measuring image quality. Many papers do have comparison of a few of the metrics. Lin Zhang's paper (Lin & Xuanqin) has by far the most comprehensive evaluation of a long list of metrics PSNR (Peak Signal to Noise Ratio), MSE (Mean Squared Error), SSIM (Structural Similarity Index), Visual Information Fidelity (VIF), Visual SNR (VSNR), Noise Quality Measure (NQM), Feature Similarity Index (FSIM/$FSIM_{c)}$, Information fidelity criterion (IFC) and many more.

The conventional metrics, such as peak signal-to-noise ratio (PSNR) and mean-squared error (MSE) focus only on the image intensity. They do not take into account the viewing person's visual experience. We can have an image which has MSE close to zero and very high PSNR but the image can be still quite blurred and be unpleasant to watch for the human eye. Thus many efforts have been made on designing human visual system (HVS) based image quality assessment metrics. These models take into account the importance of the sensitivity of HVS to visual signals like luminance, frequency content and contrast. The noise quality measure (NQM) and the visual SNR (VSNR) are two such HVS based metrics. Structural similarity (SSIM) index addresses the loss of structure in the image. Human eye is highly tuned to extract the structural information from the visual scene. Thus SSIM evaluation should provide a good measure of the perceived image quality.

Information fidelity criterion (IFC) for IQA (Image Quality Asssessment) quantifies the information shared between the distorted and the reference images. IFC was later extended to the visual information fidelity (VIF) metric. There were also studies conducted which made use of the complex wavelet (CW) transform to measure the SSIM of the two images and proposed the CWSSIM index. Feature Similarity Index (FSIM) was later proposed for IQA. FSIM depends on Phase Congruency (PC) and Gradient Magnitude(GM) of the image. The tests carried out by Lin Zhang gives us an idea of the better suitability of FSIM for IQA.

For the purpose of this paper, we have selected three out of the above list of metrics MSE, PSNR and FSIM. The equations for the evaluation of these metrics as well as brief explanation of the terms are given in the subsections below:

4.1 PSNR and MSE

Peak signal-to-noise ratio (PSNR) is the ratio between the maximum possible power of a signal and the power of distorting noise that affects the quality of the signal. Because signal values vary in applications (the difference between the smallest and largest values possible is significant) logarithmic decibel scale is used to express PSNR. The mean squared error (MSE) is used to compare the original image and the noisy image. The noise in the image can be introduced either during the transmission or during the processing done on the image (encoding, encryption, adding watermarks and so on). MSE is the average of the squares of the errors between the actual image and the noisy/processed image. MSE is the amount by which the original image differs from the degraded image. The aim is to minimize the error as much as possible thus making PSNR as high as possible. The mathematical equation of PSNR is as follows:

$$PSNR = 20\ \log_{10}\left(\left(MAX_f\right)/\sqrt{MSE}\right) \tag{1}$$

Where MSE (Mean Squared Error) is

$$MSE = \left(\frac{1}{mn}\right)\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}\left(\left(f(i,j) - g(i,j)\right)\right)^2 \tag{2}$$

(a) *f* represents the matrix data of our original image

(b) *g* represents the matrix data of our watermarked image in question

(c) *m* represents the numbers of rows of pixels of the images and *i* represents the index of that row

(d) *n* represents the number of columns of pixels of the image and *j* represents the index of that column

(e) MAX_f is the maximum signal value that exists in our original known to be good image

The MSE between two identical images will be zero and hence the PSNR will be infinity. The limitation of using only MSNR and MSE as metrics is that an image with high PSNR and very low MSE with respect to the original image can still appear blurred to the human eye. For color images, the MSE is taken over all pixels values of each individual channel and is averaged with the number of color channels. Another option may be to simply perform the PSNR over a converted luminance or grayscale channel as the eye is generally four times more susceptible to luminance changes as opposed to changes in chrominance. This approximation is left up to the experimenter.

4.2 FSIM

PC is used as the primary feature in computing FSIM and the image gradient magnitude (GM) is computed as the secondary feature to encode contrast information. These two parameters complement each other. Although FSIM is designed for grayscale images, the chrominance information can be easily added to calculate $FSIM_c$.

To compare two images I1 and I2, we first calculate the similarity score for their PC and GM individually. The similarity measure for $PC_1(x)$ and $PC_2(x)$ is defined as

$$\mathrm{S_{PC}(x)} = \frac{(2\mathrm{PC_1(x).PC_2(x)+T_1})}{\mathrm{PC_1}^2\mathrm{(x)+PC_2}^2\mathrm{(x)+T_1}} \tag{3}$$

where T1 is a positive constant to increase the stability of SPC.

The similarity measure for the gradient magnitude $G_1(x)$ and $G_2(x)$ is defined as

$$\mathrm{S_G(x)} = \frac{(2\mathrm{G_1(x).G_2(x)+T_2})}{\mathrm{G_1}^2\mathrm{(x)+G_2}^2\mathrm{(x)+T_2}} \tag{4}$$

where T2 is a positive constant depending on the dynamic range of GM values.

Similarity $S_L(x)$ at each location x is defined as $S_L(x) = S_{PC}(x) * S_G(x)$. To calculate the overall similarity between I1 and I2 we need to do more than a simple summation. This is due to the fact that human visual system gives varied importance to the different parts of the image. The edges matter more than the smooth areas within an image. PC at a given location decides the way at which HVS views it. As we are comparing two images we have to take into account the PC value at both images at a given location. The maximum of these two values will decide the impact on HVS.

$PC_m(x) = max(PC_1(x), PC_2(x))$ is used to to weigh $S_L(x)$. FSIM index between I1 and I2 is defined as

$$FSIM = \frac{\sum_{x \subset \omega} S_L(x).PC_m(x)}{\sum_{x \subset \omega} PC_m(x)} \quad (5)$$

5. Watermarking Using Bit Plane Allocation

Watermarking involves adding an image to the content in order to ensure ownership of data. Mostly the watermark is not visible to the human eye but can be detected by proper software. There are various ways in which watermarking can be implemented. Additive watermarking achieves watermark in spatial domain by adding pseudo random noise pattern to the intensity of image pixels. Adding the watermark to the LSB is a popular and simple technique but not very robust. Spread spectrum modulation based watermarking technique combines the host image linearly with a small pseudo noise signal that is modulated by the embedded watermark.

In the method followed in this paper watermarking using bit plane allocation, suggested by Gwanggil Jeon, is used (Jeon, 2014). Adding the watermark in the LSB (Least Significant Bit) is not very robust. During processing or transmission there is a possibility of the LSB getting removed or corrupted. Adding the watermark in the MSB (Most Significant Bit)is not an option as it degrades the visual quality of the image. The task at hand is to find the optimum bit plane where the watermark can be added. The steps involved are listed below:

(a) The watermarking symbol is obtained from the user

(b) The given image has to be sliced into the different bit planes. Black and white images will be sliced into 8 planes. Color images are divided in to R,G,B planes each of which will be sliced into 8 bit planes.

(c) In the case of black and white images - the metrics PSNR, MSE and FSIM are calculated separately after adding watermark individually to each bit plane. The results are tabulated and the optimum bit plane for adding the watermark is finalized taking into consideration all the metrics.

(d) In the case of color images, there will be a total of 10 metrics to consider. PSNR for R/G/B and CPSNR RGB form the four metrics. Similarly MSE for R/G/B and MSE RGB form the next four. FSIM and $FSIM_c$ are the last two metrics.

(e) Add the watermarking symbol to each bit plane and determine the value of each of the metrics mentioned above.

FSIM and PSNR were calculated individually for each of the bit planes in which the watermark was inserted. We finally zeroed in on inserting the watermark on bit plane number 4 after considering all the metrics - peak signal to noise ratio, mean squared error and feature similarity index. The watermarked image with the watermark added in bit plane number 4 produced an FSIM of 77.4% which is assumed to be an optimal value. The two images given in the figures 2 and 3 show the inserted watermark on the two respective bit planes. Adding the watermark in MSB makes it quite visible to the human eye whereas the optimal bit plane number 4 gives better results.

Figure 1. Original Image

Figure 2. Image with watermark in MSB plane

Figure 3. Image watermarked in bitplane 4

6. Image Encryption

Encryption of data is performed before transmission on an open network to make sure that only the intended user can decrypt and extract the data. Data can be either messages or images. The goals of encryption are confidentiality, authentication, data integrity and access control. There are different methods in which image encryption can be done (Ambika, Himanshu, & Anurag, 2014). In the case of symmetric cryptography the receiver uses the same key as the sender to decrypt the image. In asymmetric cryptography there are two keys – one which is public and another which is private. This key pair is mathematically linked. Asymmetric cryptography is also known as public key cryptography. Public key is published. The private key generation from the public key is computationally so difficult that it can be assumed to be impossible to do so. Some of the popular techniques are

(a) Combined symmetric cryptography using relative displacement and dynamic base transformation.

(b) Combination of block displacement and block cipher technique

(c) RGB pixel transposition and shuffling based technique

(d) Technique based on explosive inter pixel displacement of RGB attribute of a pixel

(e) Permutation based image encryption technique

In this paper we do a sequence of operations based on the RSA hash. RSA is a public-key cryptosystem. In RSA, the encryption key is public and differs from the decryption key which is kept secret. The RSA algorithm consists of key generation, encryption and decryption. The public key is accessible to everyone and it is used for encrypting messages. Messages encrypted with the public key can only be decrypted in a reasonable amount of time using the private key. The keys for the RSA algorithm are generated the following way:

(a) Choose two distinct prime numbers p and q.

(b) Compute $n = pq$.

(c) $\psi(n)$ value is kept private. Compute $\psi(n) = \psi(p) * \psi(q) = (p-1)(q-1) = n-(p+q-1)$, where ψ is Euler's totient function.

(d) Choose an integer e such that $1 < e < \psi(n)$ and e and $\psi(n)$ are co-prime.

(e) Solve for d given $d * e \equiv 1 * (mod\ \psi(n))$

The public key consists of the modulus n and the public (or encryption) exponent e. The private key consists of the modulus n and the private (or decryption) exponent d, which must be kept secret. p, q, and y(n) must also be kept secret because they can be used to calculated.

RSA's biggest advantage is that public key is not enough to decrypt the message. RSA can also be used to "sign" a message so that the receiver can be sure that the message originated from the actual sender.

The following steps are followed in our algorithm. The image is divided into blocks .Following a division of the image into 10x10 blocks, we randomly move the image around and assume the receiver has knowledge about the manner in which the image is moved.

Figure 4. Original Image

Figure 5. Moved Image

Figure 6. Hashed Image

The figure 4 and 5 show the original image and the moved images. An alternative way is to use a PRNG with the same seed at both the sides. In this paper, hashes are done are on 10x10 blocks. The hashed blocks together form the hashed image which is stored for further processing. More than 117 bytes cannot be hashed. Hence we settle for the 100 bytes from the 10x10 blocks for hashing. It is to be noted that the two images are of different sizes. This is because the original image is re-sized prior to the encryption. The reason this operation is performed is whenever a secret image is to be hidden in a cover image, the cover image must always be larger. In order to reduce the size of the secret image, we re-size it before hashing.

7. Steganography

In Steganography the hidden image appears to be a part of the cover image. There have been several different ways in which Steganography has been performed previously. In LSB embedding only the LSB is changed. This requires the cover image to be much larger than the original image. However, it affects the appearance of the image to a minimal extent. Further research and surveys are available at (Image Steganography and Steganalysis) on different methods of steganography. In this paper we use DCT (Discrete Cosine Transform) is used to hide the secret image within the cover image. The general quantization matrix for the DCT that is as follows

$$M = \begin{matrix} 3 & 5 & 7 & 9 & 11 & 13 & 15 & 17 \\ 5 & 7 & 9 & 11 & 13 & 15 & 17 & 19 \\ 7 & 9 & 11 & 13 & 15 & 17 & 19 & 21 \\ 9 & 11 & 13 & 15 & 17 & 19 & 21 & 23 \\ 11 & 13 & 15 & 17 & 19 & 21 & 23 & 25 \\ 13 & 15 & 17 & 19 & 21 & 23 & 25 & 27 \\ 15 & 17 & 19 & 21 & 23 & 25 & 27 & 29 \\ 17 & 19 & 21 & 23 & 25 & 27 & 29 & 31 \end{matrix}$$

DCT is used in JPEG compression. We aim to minimize the amount of redundancy introduced. We would like to decrease the size of the cover image and make it as small as possible. The LSB approach mentioned earlier requires 1 pixel for storing 1 bit of information. Our approach to this to steganography is slightly different.

Table 1. Algorithm for Steganography

Step	Action
1:	Procedure START
2:	DCT has both +ve and -ve values the original image is subtracted from 128(for an 8 bit)
3:	Normalize the above image
4:	We find an optimal location for inserting the secret pixel. The criteria is that the difference should be as minimal as possible

Note. The algorithm followed by this paper is detailed in the table below. The image has to be normalized first before inserting the secret pixel.

- From the DCT which is computed on the 8X8 blocks, we first convert it into n number of arrays each of size 64 and then find the closest match based on the above mentioned condition and insert the pixel at that location. The location of the pixel is noted. The main advantage of this form of direct insertion is that the original image need not be much larger than the cover image as required for traditional techniques. One disadvantage is that the locations at which the data is inserted must be known before hand. But this is generally a problem which is specific to most Steganography techniques. The location of the pixels in the DCT is assumed to be known by the receiver. However, if this knowledge is not known before hand, the pixel locations once again can be hashed and shared without compromising the security of the data transmission.
- Another way is to use neural networks to identify the area in which the pixel must be inserted. The main challenge involving the neural network is the generation of the training pattern. In order to generate this training pattern we insert the pixels of the secret image at random location and determine the value of FSIM. The maximum value of FSIM is determined. The pixels of the secret image are then input to the neurons and the target is the pixel location at the DCT. This involves extensive training and is the best method. However in this paper we do not explore this proposal. The author is working on using Neural Networks to identify pixel location is Steganography.
- If the FSIM requirement is very high then neural network can be used.

Figure 7. 3 different images can be hidden inside one image

Figure 8. Cover Image used for Steganography

Figure 9. Decrypted images from the cover image

8. Conclusion

The features of watermarking, image encryption as well as image steganography were combined before transmitting the data. The required watermark was inserted on the image at the optimum bit plane. RSA hash was used to encrypt the image. The encrypted image was then hidden within a selected cover image. A set of metrics were used for evaluation of the effectiveness of the approach. As shown in the results above the combining of these three areas resulted in a reliable and secure data transmission.

References

Ambika, O., Himanshu, Y., & Anurag, J. (2014). Review: Image Encryption Techniques and its Terminologies. *International Journal of Engineering and Advanced Technology , 3*(4).

Dobsicek, M. (2014). Extended steganographic system. *8th Intl. Student Conf. on Electrical Engineering.*

Emam, N. (2007). Hiding a Large Amount of Data with High Security using Steganography algorithm. *Journal of Computer Science* .

Image Steganography and Steganalysis. (n.d.). Retrieved from http://www.ims.nus.edu.sg/Programs/imgsci/files/memon/sing_stego.pdf

Jeon, G. (2014). Watermarking Application Using Bit Plane Allocation. *International Journal of Security and its Applications , 8*(5).

Lim, Y., Xu, C., & Feng, D. D. (2001). Web based image authentication using invisible fragile watermark. *VIP2001*.

Lin, Z., & Xuanqin, M. (n.d.). Retrieved from *http://www4.comp.polyu.edu.hk/~cslzhang/IQA/TIP_IQA_FSIM.pdf*.

Rehab H, A., Fadhil J, K., & Ahmad T, A. (2005). Data Embedding Based on Better Use of Bits. *International Journal of Signal Processing 2005.*

SK, B., Debnath, B., Swarnendu, M., Debashis, G., & Poulami, D. (2008). A secure scheme for image transformation. *IEEE SNPD.*

Wu, M., & Liu, B. (2004). Data Hiding in Binary Image for Authentication and Annotation. *IEEE Trans. Image Processing, 6*(4), Aug. 2004.

Youssra, L., & Mohammed, E. (2013). A comparative study of some images watermarking algorithms. *International Journal of Digital Signal and Image Processing.*

Copyrights