Matrix Academic International Online Journal Of Engineering And Technology
© MAIOJET
ISSN: 2348 – 3326

Digital Watermarking Using Color Image Processing Using images for transmitting secret information

Achal Kumar[1], Vibhav Prakash Singh[2]

Department of Computer Science & Information Technology
Anand Engineering College, Agra, India.

achaltomar@gmail.com, vibhav.gla@gmail.com

Abstract –Digital watermarking can be used for transmitting secret information, by embedding that information into the images. This paper presents a technique to implement information hiding in color images using Advanced Encryption Scheme (AES-128) and Secure Hash Algorithm (SHA-512) to give a time effective algorithm. AES-128 is used to encrypt the message and SHA-512 is used to provide message authentication. Some experimental values are also given in this paper to show the effectiveness of proposed technique.

Keywords-Digital Watermarking, cryptography, information hiding, color model, message authentication code.

I. INTRODUCTION

In the recent years, there is a huge change comes in the way of seeing and using images. Analog form of multimedia was practically replaced by the digital form of multimedia almost in the all areas of the human life. The reasons for using digital images in spite of analog are the property of easy copying and the efficiency gained in transmitting them. Another reason for using digital images is the increment in using image transfers via different types of network.

Digital watermarking is process of embedding additional information directly into the digital multimedia, also called original data, by making small modifications to them.

Digital watermarking technologies allow users to embed digital code into images and video which are imperceptible during normal use but readable by computers and software. The additional information is called watermark.

Generally watermarks are used where authentication or ownership is needed. Watermarks are a good way by which anyone can prove that the multimedia is related to him. Also, watermark can be used to transmit secure message from one to other party, both satisfying to use same technique. Watermarks used should be invisible, in the sense that, they are embedded into the image after implementing any cryptographic algorithm. Being the need of more security, the authentication can also be used. Authentication can be provided by using Message Authentication Code, and embedding this code into the image too. The problem comes here is the computational cost and time complexity of using a robust cryptographic algorithm with some authentication code algorithm.

Till now, the techniques were using the concept of message authentication code only. Those techniques were ensuring that if there comes any change in the message, it will be caught as, when the authentication code calculated with the corrupted message, it will not match the one which is in image. Suppose the case when intruder not wants to alter the message, in spite he just wants to take the message, like copying password. At this time, the previous technique fails, as the message is in plain text. So, a technique should be proposed, which uses both message security, i.e., confidentiality [10] and message authentication i.e., integrity [9]. This paper proposes such a technique. When digital watermarking is used to transmit a secret message, there are several attempts which are made by intruders to recognize the secret message. This is called as attack [10] on image being transmitted. The attacks may be categorized in two categories, one is passive attacks [10], in which the message content is not modified, second is active attacks in which the message content is also modified [10]. There are several types of attacks being possible:

- Masquerading
- Replaying
- Denial of Service
- Fabrication
- Spoofing

But here the main concern should be about how to protect the secret information which is being transmitted by embedding into the image.

As now days, the more concern is of security with less time complex algorithm to be use in encryption. If any heavy algorithm like RSA will be used, then the computation cost will raise to the sky, and if any low order algorithm is used, the security will down below the earth. Thus, a computationally cost and time effective technique should be implemented, which guarantees the security of message.

The remaining sections of the paper include:

Section 2: Proposed Watermarking Method

Section 3: Applications and Efficiency Measurement

Section 4: Experimental Results

Section 5: Conclusion

II. PROPOSED WATERMARKING METHOD

As each intensity value in color images ranges from 0 to (2^{24}-1), and from 0 to (2^8-1) in each of the three components of color image as RED, GREEN and BLUE [8]. Also each character have there ASCII values ranges from 0 to (2^8-1).So,

any text can be embedded into the image, by replacing the intensity value of any component at that pixel location, with the ASCII value of character [7], which is needed to be transmit. Hence, first applying any cryptographic algorithm to text, and then embedding the resulting ASCII to image, will provide the necessary security.

The key idea to implement this technique is to propose an algorithm which can be used to embed secret message into the image in a computational and time effective manner. Instead of using a heavy cryptographic algorithm like RSA [10], an effective algorithm like AES [10] can be used with authentication scheme like SHA [9]. The proposed technique consists of two sections. First is how to embed a text into image, i.e., Watermark Embedding. Second is how to extract the secret message from the watermarked image. The technique also discusses how and where to place the authentication code in an image.

1. Watermark embedding

The input to the algorithm is original image I, watermarked image WI, secret message p and 128 bit key, k used in AES-128 encryption scheme. The second phase of watermark embedding includes another input iv, initial value, which is 512 bits long, and used for the purpose of generating 512 bits long message authentication code m, which is also embedded into the image. The process of watermark embedding is shown in figure 1 and can be described in following two phases:

Phase I: Calculation of all parameters

• Calculate the cipher text, c, by using p, k and AES-128 encryption scheme. It will be implemented using block cipher.

• Calculate message authentication code, m, using p, iv and SHA-512 scheme. Notice here that, m is generated by using plain text p, not by using the cipher text c. This will confuse the intruder, and the technique will be more secure.

• Calculate positioning pixels as:

Row positioning pixel, r' = I(1,1)+1

Column positioning pixel, c' = I(1,2)+1

Phase II: Placement of cipher and authentication code into image

• Replace the pixel value starting from (r', c') in the original image with the value of cipher text c. Each block in cipher text will change exactly 16 pixel bits in the original image.

•Replace the last 64 pixel bits, with the authentication code calculated, in reverse order. This will enhance the intruder confusion.

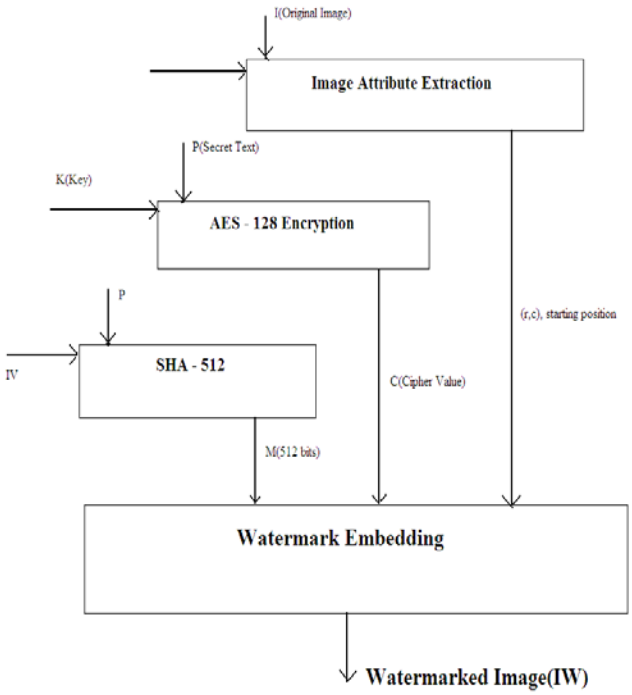

Figure 1. Watermark Embedding

2. Watermark extraction

The watermark can be extracted from the watermarked image by using the inverse procedure of above scheme. This is shown in figure 2 and will also proceed in two phases:

Phase I: Point out the placement of cipher and authentication code

• Calculate the r' and c' values, and then point out the starting position of c in watermarked image WI.

• The authentication code m is in the last 64 pixels and is in the reverse order.

Phase II: Calculation and verification of secret text.

• Secret text, p is calculated by using k and AES-128 decryption algorithm.

•Verification of p as a correct message is done by calculating authentication code m' from p. If m and m', both are equal, the extracted message is correct.

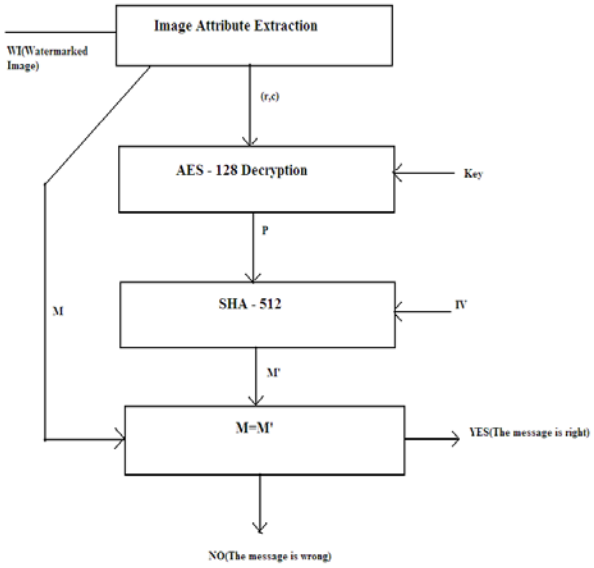

Figure 2. Watermark Extraction

III. Applications and Efficiency Measurement

As discussed so far, embedding secret message into images and then use to transmit images to share secret message, is a good method to be used in the case when the message is not very long in size. This is because when the message is short, the change made to the original images is also short, resulting in less change in original image, and hence intruder will not be able to catch the secret. The proposed technique can be used in every type of image such as Binary images, Gray scale images and Color images. By end, it can be said that this technique is best suited to transmit symmetric keys in secure manner.

The technique is very economical, because it uses light cryptographic algorithm AES-128 with SHA-512 to provide double security with half computational time. The reason for this is that, if RSA is used then it leads to two major problems. One is its key length is very high, i.e., of 1024 bits, it will be more difficult to calculate exponential computations than simple computations needed in AES which uses the key of length only 128 bits long. Also, the technique proposed in this paper uses the mixing concept to generate message authentication code, and put it in reverse order to confuse the intruder. It will give more effective results when the complex images are used. One more point to be notice is that it will give best results when the used images are of PNG (Portable Network Graphics) format, which possess the property of lossless data compression.

IV. Experimental Results

The experiment have been done by using RGB color model, with the group of thirty five different types of images, some taken from Internet [5], some from Digital Camera, and some from 'Print Screen' functionality. The influence of the embedded watermarks into the different color components of the color model are measured by PSNR (Peak Signal to Noise Ratio) and the average values for every color component are presented in the TABLE 1.

TABLE 1. PSNR Values.

Color Component	PSNR[dB]
R	54.55
G	51.98
B	51.23

As can be seen from the table, the different values were obtained by using different color components of the color model. It can also be derived that for modifying X color component of the image, if the image having X color component in majority, is used, the watermark will be more invisible, where X is any color component from RED, GREEN and BLUE component of RGB color model.
There are also some samples PNG images are displayed in Appendix 1(images A, B, C, D, E) which were used for making experiment successful.

V. Conclusion

The proposed technique will provide better security against both types of attacks, i.e., active and passive attack, and also results in computationally cost effective algorithm by using light algorithm with message authentication code. The proposed technique will work more efficiently on PNG images, because of there lossless compression property. Hence, it can be said that, the technique is a useful one, for transmitting secret information via images.

References

[1] Ridzoň, R.; Levický, D.: "Robust Digital Watermarking in Color Images" vol. 16, no. 4 (2007), p. 76-81.

[2] Ridzoň, R., Levický, D.: "Robust image watermarking based on the synchronization template". In: Radioelektronika 2008: 18h international Czech - Slovak scientific conference, April 2008, Praha, Czech Republic.

[3] Voloshynovskiy, S. et al.: "Attack Modeling: Towards a Second Generation Watermarking Benchmark", Sig. Processing, Special Issue on Information Theoretic Issues in Digital Watermarking, 2001, vol. 81. no. 6, pp. 1177-1214.

[4] Halftone Image Watermarking based on Visual Cryptography.
[5] Digital Image Processing, Gonzales and Woods, Third Edition.
[6] Network Management and Security, B. Forouzan, Special Indian Edition.
[7] Cryptography, William Stallings, Third Edition.
[8] Deguillaume, F.; Voloshynovskiy, S.; Pun, T.: "A method for the estimation and recovering from general affine transforms in digital watermarking applications", In Security and Watermarking of Multimedia Contents IV, pp. 313–322, 04/2002
[9] Ridzoň, R.; Levický, D.: Robust digital watermarketing based on the log-polar mapping. In: Radioengineering. vol. 16, no. 4 (2007), p. 76-81.
[10] Ruanaidh, J.J.K., Pun, T.: "Rotation, scale and translation invariant digital image watermarking", in Proc. IEEE Int. Conf. Image Processing 1997, Santa Barbara, CA, vol. 1, pp. 536–539, Oct. 1997.

Appendix 1. Some Sample Images

A B C

D