Rikki Sharma, Priyanka Surve, Mrs. Devyani Bonde / International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com
Vol. 3, Issue 3, May-Jun 2013, pp.1236-1238

STEGO-WATERMARK

Rikki Sharma, Priyanka Surve and Mrs. Devyani Bonde
(Department of Information Technology, Pune University, Pune-47)
(Department of Information Technology, Pune University, Pune-47)
(Department of Information Technology, Pune University, Pune-47)

ABSTRACT

The evolution of the Internet helps the transmission of digital multi- media content such as text, audio, images, and video easier. Digital media can be accessed or distributed through the network. As the communication over internet is easier and convenient, the security becomes main concern. One of the approaches for secured transmission is Steganography in which secrete message is hidden behind the image. For authenticity, digital watermarking is a technique which embeds a digital signature or digital watermark that asserts the ownership or intellectual property rights of the owner .In this a hybrid approach is used, in which watermarking and Steganography techniques have been combined, which exploits the advantages of both techniques results in more robustness against different types of attacks.

Keywords - *Robustness, Steganography, Watermarking.*

1. Introduction

To protect and enforce intellectual property rights of the media owner is an important issue in the digital world. Digital Watermarking works by concealing information within digital data, such that it cannot be detected without special software with the purpose of making sure the concealed data is present in all copies of the data that are made whether legally or otherwise, regard-less of attempts to damage/remove it. In addition to it, Steganography is the art and science of writing hidden messages in such a way that no one, apart from the sender and intended recipient, suspects the existence of the message, a form of security through obscurity. Image Steganography allows for two parties to communicate secretly and covertly. Thus an image can be the source of medium to transfer the secret data from one place to another and it also refers the ownership rights by using both these technique. The technique given by Tsung-Yuan Liu and Wen-Hsiang Tsai[1] uses Visible watermark. The advantage of this technique is it gives lossless recovery of image. But being visible the watermark can be pose threat easily. The technique used by Satya Prakash Sahu,Satya Verma [2] of LSB replacement for Steganography in which data is hidden in the LSB part of the image and visible watermarking with Opacity factor in which the watermark remains visible with the opacity factor which controls the transparency. But the technique fails to provide security to hidden data as it is hide in the LSB part, which can easily affected. Also it uses two keys one for the Steganography.

The technique used in this paper follows the approach used in above method [2] but the algorithm BPCS Steganography(Bit Plane Complexity)[3] is used for implementing Steganography and Alpha channeling for watermarking.

2. Concept

2.1 MESSAGE AND WATERMARK EMBEDDING

1. Carrier image is first loaded. The image should be in 24 bpp. Secret data is the data which is to be embedded into the Carrier Image.
2. The secret data can be encrypted by applying Key to the encryption process and then data is embedded into the carrier image.
3. The image obtained by applying BPCS Steganography algorithm in which carrier image is divided into 8 by 8 blocks and secret message is embedded into the particular block depending upon the complexity.
4. If user wants to extract some data in between the process, then he can extract the same from the Steganographic Image.
5. Watermark is embedded into the Steganographic Image with the help of alpha channeling. Alpha channel is an extra 8 bits added to the 24 bpp Carrier Image which contains the Author data.
6. Final Stego-Watermark Image is the final image obtained after applying Steganography and Watermarking.
7. This image contains the Author data which is either encrypted or embedded as it is. Also it contains the Watermark for Tamper detection to the author data.

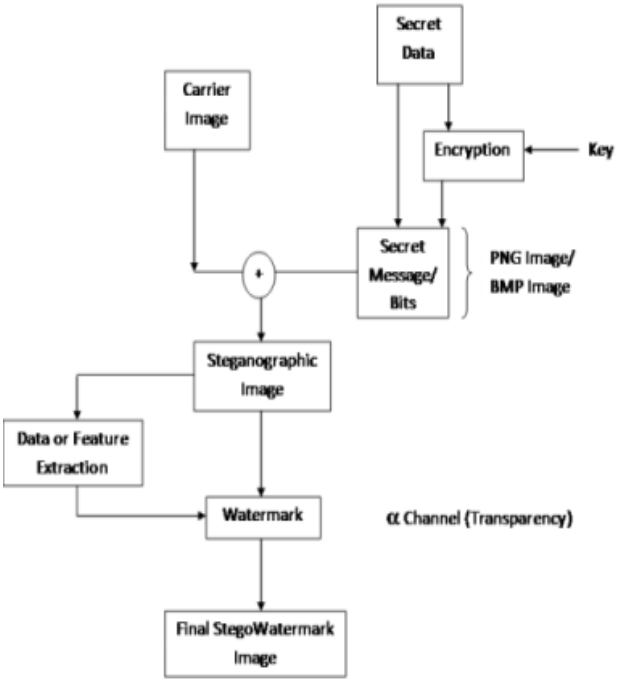

Figure 1: Message And Watermark Embedding

2.2 MESSAGE AND WATERMARK EXTRACTION

1. At the detection stage first extraction of the watermark from Stego-Watermark image is done.
2. At verification and analysis phase, verification of watermark and original Stego-image is done, to detect the changes or damages if occurred. Watermark verification, Alpha channel verification and verification of Carrier image will be done in analysis phase.
3. At BPCS De-Steganography stage, BPCS De-Steganographic algorithm is applied to the Steganographic Image.
4. Original data is extracted depending upon the complexity values of the different blocks of the carrier image.
5. If the data is encrypted, it is decrypted with the help of specific Key to get the Actual Data.

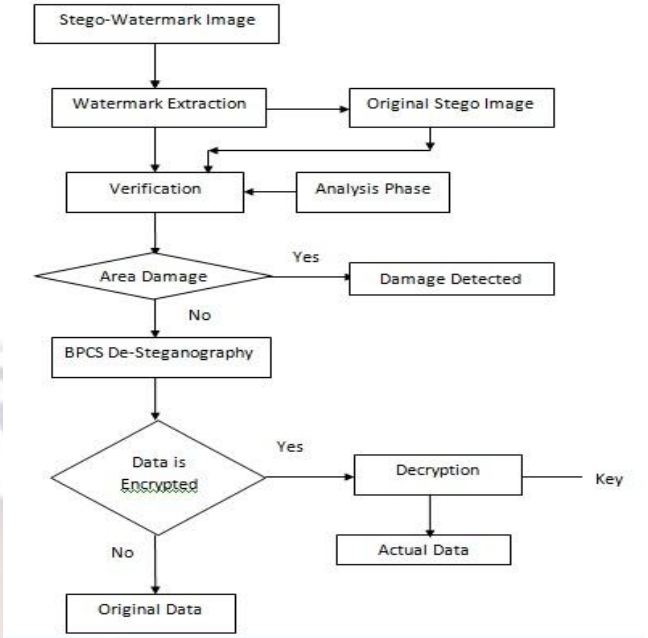

Figure 2: Message And Watermark Extraction

3. Proposed System

3.1 BPCS STEGANOGRAPHY

The BPCS Steganography technique divides the Carrier Image (Image that needs to be transmitted) into 8 by 8 blocks and there is high correlation between these blocks. The higher the block is, the stronger the correlation between the pixels of the blocks. The complexity of each block is calculated. The maximum complexity value is Cmax. The threshold complexity value is set to aCmax. The block containing the value higher than the aCmax is replaced by the secret data which is either encrypted or not.

3.2 ALPHA CHANNEL FOR WATERMARKING

The alpha channel masking algorithm is used improve the robustness and protection along with security. Alpha channel is an additional channel which contains the information regarding the image transparency and its various level. It is an extra 8bit channel other than RGB channels which controls the transparency. In this intermediate image data (grayscale component of the intermediate image) itself as the data to be watermarked on the intermediate image is used. This data will helps to determine if there is any modification or damage done to the original image and also reconstruct the original image to some extent.

3.3 BASIC ALGORITHMS

3.3.1 MESSAGE EMBEDDING USING BPCS

1. Divide the carrier image into 8 by 8 blocks and calculate the complexity.
2. Maximum complexity is calculated.

3. Compare calculated complexity with threshold complexity.
4. The secret data is either encrypted or not encrypted.
5. Embed the secret data in the block if the complexity greater than maximum complexity.
6. If complexity is less than maximum complexity then conjugate another block to make it more complex.
7. If conjugate process is involved, make an entry for the same in conjugate map and embed it in Carrier image.

3.3.2 MESSAGE EXTRACTION USING BPCS

1. Pick up all the pieces whose complexity greater than maximum complexity.
2. For confirmation of conjugate blocks pick up the extra information.
3. Blocks are then decrypted to get the original message.

4. Conclusion

In this System, the different aspects and issues of these techniques are focused. The watermarked Steganographic image is communicated over the non secure network. By this approach, not only the secured and authentic mode of transmission for textual message is achieved but also the user can detect the changes or damages done to the watermark and the carrier image. At last, this technique uses better methods than previous system for applying Steganography and Watermarking for providing security to the user's data.

REFERENCES

[1] Tsung-Yuan Liu,Wen-Hsiang Tsai "*Generic Lossless Visible Watermarking (IEEE Journal).*"

[2] Satya Prakash Sahu, Satya Verma. "*Computer Networks and Information Technologies. (Second International Conference)*.Year: March 2010-11."

[3] Pei pei Shi,Tao Zhang "*A Technique of Improved Steganography using BPCS And Chaos*(IEEE Journal 2010)."

[4] ZHANG H L, ZHANG X Y. "*A secure BPCS Steganography against statistical analysis"*. 8th International Conference on Signal Processing. 2006: 990-992."

[5] Hioki H.A "*data embedding method using BPCS principle with new complexity measures"*. Pacific Rim Workshop on Digital Steganography,2002.

[6] Wei, H., Yuan, M., Zhao, J., Kou, Z. "*Research and Realization of Digital Watermark for Picture Protecting"*. In: First International Workshop on Education Technology and Computer Science (2009).