ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

*(An ISO 3297: 2007 Certified Organization)*

**Vol. 4, Issue 2, February 2016**

# Improved Copyright Image Protection using Steganography Technique

Sanchit Mahajan

M.E. Student, Dept. of C.E., D.P.C.O.E. Wagholi, Pune, Maharashtra, India

**ABSTRACT:** The protection of data can be done by several mechanism to secure and achieve authenticity and integrity of data. Data hiding is a technique in which a piece of information can be embedded to cover media data for security reason. So a digital watermarking can be used to protect the copyright of digital products. In such processes it is needed to maintain the original view of the host image. For evaluating the watermarking methods performance it must be concentrate on the robustness of watermarked image quality and restored image quality. For this purpose the steganography encoding mechanism can be used. So a steganography code can address the next level of protection to perform various procedures for the sake of integrity and security.

**KEYWORDS**: Digital Watermark, Steganography.

## I. INTRODUCTION

To protect the legal copyright of diverse forms of multimedia, techniques used to embed information are desperately needed. The data hiding techniques focus on how to efficiently embed a piece of information into cover media data to carry out specificmissions. Often used in pairs in this emerging field, digital watermarks have shown promise in protecting the copyright of digital products.

The embedding watermarks into the original host image involves two key tasks - confirming copyright protection and maintaining the original view of the carrier image. To protect the copyright of an image, a watermarking mechanism must be robust enough to resist malicious attacksthat is, an authorized user must be allowed to retrieve a recognizable information, even if the watermarked image has been attacked by various methods.

Furthermore, the watermarked images quality must be good so that it is difficult for an intruder to distinguish between the host image and the embedded one. In addition, the embedded information should not seriously distort the protected image, which may degrade the images value. Thus, when evaluating a watermarking mechanisms performance, we have to concentrate on three issues: robustness, the watermarked images quality, and the restored information quality.

## II. RELATED WORK

To enhance our scheme's robustness and guarantee the least impact on the embedded images, in [1] Jung-San Lee et.al.,used a preinserted encoding method in the discrete cosine transform (DCT) domain to accomplish the embedding and extraction procedure. In addition to resisting various malicious attacks, our method requires minimal information to extract the embedded watermark and restore the host image with high quality. To help describe the method, we use a simulator preinserted code (PIC) to perform all the procedures.

A.M. Alattar in [2] used a very high-capacity algorithm based on the difference expansion of vectors of arbitrary size developed for embedding a reversible watermark with low image distortions. A reversible watermarking algorithm with very high datahiding capacity has been developed for color images. The algorithm restores the exact original image, hides several bits.

In [3] C.C. Chang et.al., presented a lossless and reversible steganography scheme for hiding secret data in each block of quantized discrete cosine transformation (DCT) coefficients in JPEG images. This shows that the two successive zero coefficients of the medium-frequency components in each block are used to hide the secret data. Also it modifies the quantization table to maintain the quality of the image.

C.C. Chang et.al., in [4] presented a reversible data hiding scheme based on side match vector quantization (SMVQ) for digitally compressed images. With this method receiver performs two steps to achieve - extract the secret data and reconstruct the original SMVQ compression codes.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

*(An ISO 3297: 2007 Certified Organization)*

**Vol. 4, Issue 2, February 2016**

M.U. Celik et.al., in [5] presented a novel framework for lossless authentication watermarking enables zero-distortion reconstruction of un-watermarked images upon verification. They presented a new lossless image authentication framework which offers computational efficiency, public/private key support and improved tamper-localization accuracy.
In [6] C.C. Chang et.al., proposed a novel watermarking mechanism by utilizing Pair difference correlations upon subsampling and the technique of JND. The simulation results revealed that the new scheme approximated a lossless watermarking scheme. Also the novel scheme resisted various signal processing attacks and geometric transformation attacks; therefore, it can be used to protect the ownership of important watermarked images.
C.Y. Lin et.al., in [7] presented an effective technique for image authentication which can prevent malicious manipulations but allow JPEG lossy compression. The authentication is based on invariance of relationships between discrete cosine transform coefficients at the same position in separate blocks of an image.
P. Bas et.al., in [8] presented a new approach for watermarking of digital images providing robustness to geometrical distortions. A new class of watermarking schemes using the image content is presented. They propose an embedding and detection scheme where the mark is bound with a content descriptor defined by salient points.
In [9] C.S. Lu et.al., proposed a scheme that can resist two famous water- mark estimation-based attacks, which have successfully cracked many existing watermarking schemes. The false negative and false positive analyses are conducted to verify the performance of scheme.
In [10] J. Barr et.al., developed a system which will mitigate the threat posed by the copy attack. They first developed an image signature algorithm which uses highly stable low frequency DCT coefficients to uniquely describe the image.
Q. Cheng et.al., in [11] presented an investigation on robust optimum detection of multiplicative watermarks. In this the novel optimum detectors for multiplicative watermarks are derived using locally optimum detection for the generalized Gaussian distributions.
In [12] C.S. Lu et.al., proposed a new digital signature scheme which makes use of an images contents to construct a structural digital signature for image authentication. For image authentication, it is desired that the verification method be able to resist content-preserving modifications while being sensitive to content-changing modifications.
S. Craver et al., in [13] addresses the capability of invisible watermarking schemes to resolve copyright ownership. They show that, in certain applications, rightful ownership cannot be resolved by current watermarking schemes alone. Specifically, it attack existing techniques by providing counterfeit watermarking schemes that can be performed on a watermarked image to allow multiple claims of right ownership.
In [14] X. You et al. proposed a new method for constructing nontensor product wavelet filter banks and applied them into watermarking scheme design. The new nontensor product wavelet filter banks are constructed according to special symmetric matrix. They overcome the drawback of tensor wavelet banks which can reveal the singularities in the three directions only.

## III. PROBLEM DEFINITION

The improved watermarking mechanism should be more efficient and robust. To develop a robust watermarking mechanism that resist malicious attacks to protect the watermarked copyright information from the original image, so an authorized user can retrieve a original recognizable watermark information, also maintaining the watermarked image quality. The watermarked image quality must be good enough so that it is difficult for an hacker to distinguish between the host image and the embedded one. Also to recover embedded watermark information even though the image is cropped up to 80 percent.

## IV. PROPOSED SOLUTION

The proposed improved protection method can improve the watermarking schemes robustness and the quality of the embedded image. Also this method can protect the watermarked information even though the image is cropped extensively. In this work we used the steganography encoding method is used to embed the watermarked copyright information into the original image, which maintains the quality of the original image. Also this is robust against various malicious attacks. For retrieving the copyrighted information from the embedded image we used the steganography decoding method that can be useful to recover the original recognizable watermarked information even though the embedded image is cropped up to 80 percent by the intruder to corrupt the copyrighted information. In

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2016

addition to resisting various malicious attacks, this method requires minimal information to extract the embedded watermark even though the image is cropped.

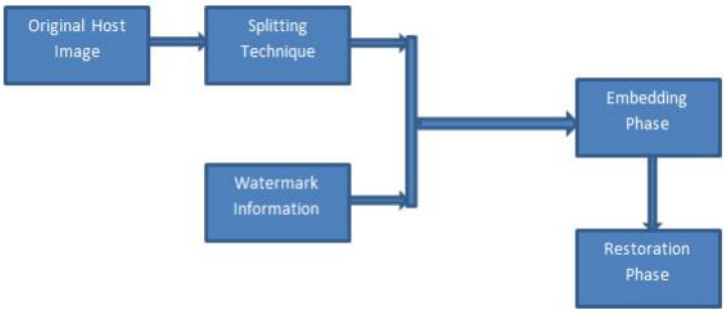


Figure 1. Different Phases Included in Proposed Work

## V. PROPOSED ALGORITHM

BEGIN:
Step 1: Select the original image and splits into 16 chunks
Step 1.1: Get Image Into ImageBuffered
Step 1.2: Get Image Dimesion
Step 1.3: Divide Image Into 16 same size parts
Step 2: Get copyright watermark message information from user.
Step 2.1: Calculate message length
Step 2.2: Convert message length into byte
Step 2.3: Convert encoding message into byte
Step 3: Convert BufferedImage into byte
Step 3.1: Get Image Dimension
Step 3.2: Get first four byte(32 bit) from image dimension and encode message lengthinto that (Using Change last bit of Byte and right/left shift bit operation)
Step 3.3: Get remaining byte of image (skip first 4 byte) and encode message intothem.(Using last bit of byte with message character and right/left shift bit operationwith message length)
Step 3.4: Apply same technique for every splited image(16 images)
Step 3.5: Get 16 encoded images and merge this image into single(Final) image
Step 4: Apply Image Splitting technique on Final encoded image
Step 4.1: Select splitted image one bye one from 1-16
Step 4.2: Get Selected Image Dimension
Step 4.3: Get first four byte(32 bit) from image dimension and decode message length(get message length) from that(Using last bit of Byte and right/left shift bit operation)
Step 4.4: Get remaining byte of image (skip first 4 byte) and decode message fromthem.(Using last bit of byte and right/left shift bit operation with message length)
Step 4.5: Get final encoded message from that
Step 4.6: Apply same technique for every splitted image(16 images)
END

## VI. MATHEMATICAL MODEL

Let S be the system that describes original image and watermark information as input to the system with splitting of original image, encoding original watermark information, embedding phase, splitting embedded image and extraction of original watermark information; this all gives output as original watermark information. Figure 2 shows illustration of mathematical model for the proposed system.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2016

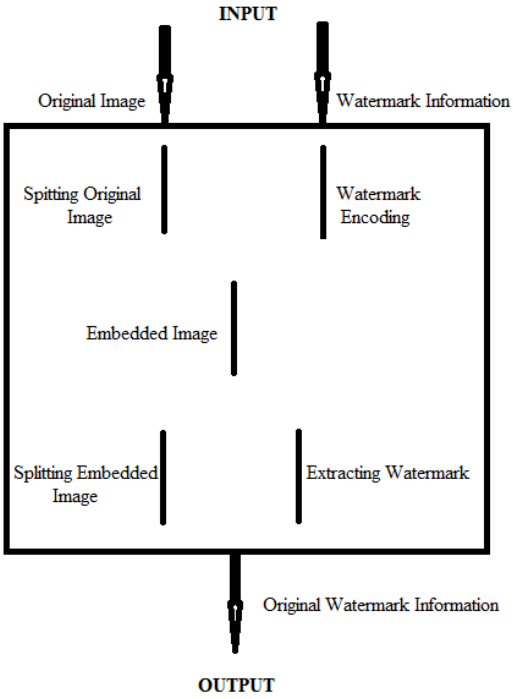


Figure 2. Illustration of Mathematical Model

$S = (S_i, S_w, D_w)$

Where S = system,
$S_i$ = Source original image,
$S_w$ = Source watermark
$D_w$ = Extracted watermark information

INPUT
$S_i$ = Source original image,
$S_w$ = Source watermark

Splitting Original Image
$S_i = (S_{i0}, S_{i1,.....}S_{i15})$
Watermark Encoding Phase
$S_{we}$= Source watermark encoding

Embedding Phase
$S_e$ = Embedding Image (Original Image + Watermark)

Splitting Embedded Image Phase
$S_e = (S_{e0,} S_{e1,.....}S_{e15})$

Extracting Watermark Information Phase
$S_{wd}$ = Source watermark decoding

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

*(An ISO 3297: 2007 Certified Organization)*

**Vol. 4, Issue 2, February 2016**

OUTPUT
The output is the original watermark information.

## VII. EXPERIMENTAL RESULTS

The work done results are shown in figures given below. Figure 3 shows the resultsof PSNR values fordifferent embedded images, which shows the efficiency of the proposed method for improving visual quality of the embedded image.

| ATTACKS | Images | Lena | | | Baboon | | | Tiffany | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | **Ratio (%)** | **10** | **25** | **75** | **10** | **25** | **75** | **10** | **25** | **75** |
| **CROPPING** | PSNR (dB) (Proposed System) | 34.7 | 34.7 | 37.33 | 31.2 | 31.1 | 35.33 | 37.3 | 37.7 | 37.88 |
| | PSNR (dB) (Existing System) | 17.35 | 12.91 | 7.51 | 16.27 | 11.32 | 5.73 | 17.83 | 11.89 | 9.87 |
| **BRIGHTENING** | **Str** | **-50** | **50** | **80** | **-50** | **50** | **80** | **-50** | **50** | **80** |
| | PSNR (dB) (Proposed System) | 18.46 | 18.46 | 15.98 | 20.6 | 20.4 | 16.2 | 18.9 | 18.2 | 16.8 |
| | PSNR (dB) (Existing System) | 16.77 | 16.57 | 15.31 | 17.38 | 16.27 | 12.55 | 15.91 | 18.84 | 16.61 |

Figure 3. Comparison of results of proposed system with existing system

## VIII. CONCLUSION AND FUTURE SCOPE

This Improved Image Protection using Steganography Techniquegenerates the improved visual quality of the embedded imageand also it is robust against various maliciousattacks. It is efficiently hides the copyright watermark information within the original image to protect the copyright of the original image.It is useful for maintaining and protecting the copyright of the digital products.The Steganography data hiding system efficiently embed the piece of watermark informationinto host media to protect the copyright of the product. The system will recoverthe watermark information even though the image is cropped up to 80 percent. Also it is helpful for sending important data within the image without affecting any quality of original. The embedded data within the host image can be recovered by only authorizedperson.
In future, further research can be done to find the best possible data hiding approach which will be more efficient and promising in terms of embedded image quality and various malicious attacks.

## IX. ACKNOWLEDGEMENTS

Sincere thanks to the reviewers for reviewing this manuscript and providing inputs for greatly improving the quality of this paper.

## REFERENCES

1. Jung-San Lee and Bo Li, Self-Recognized Image Protection Technique that Resists Large- Scale Cropping, 2014 IEEE Computer Society.
2. A.M. Alattar, Reversible Watermark Using the Difference Expansion of a Generalized Integer Transform, IEEE Trans. Image Processing, vol. 13,no. 8, 2004, pp. 11471156.
3. C.C. Chang et al., Reversible Hiding in the DCTBased Compressed Images, Information Sciences, vol. 177, no. 13, 2007, pp. 27682786.
4. C.C. Chang,W.L. Tai, and C.C. Lin, A Reversible Data Hiding Scheme Based on Side Match Vector Quantization, IEEE Trans. Circuits and System for Video Technology, vol. 16, no 10, 2006,pp. 13011308.
5. M.U. Celik, G. Sharma, and A.M. Tekalp, Lossless Watermarking for Image Authentication: A New Framework and an Implementation, IEEE Trans. Image Processing, vol. 15, no. 4, 2006, pp.10421049.
6. C.C. Chang, P.Y. Lin, and J.S. Yeh, Preserving Robustness and Removability for Digital Watermarks Using Sub sampling and Difference Correlation, Information Sciences, vol. 179, no. 13, 2009, pp. 22832293.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

*(An ISO 3297: 2007 Certified Organization)*

**Vol. 4, Issue 2, February 2016**

7. C.Y. Lin et al., A Robust Image Authentication Method DistinguishingJPEG Compression from Malicious Manipulation, IEEE Trans. Circuitsand Systems for Video Technology, vol. 11, no. 2, 2001, pp. 153168.
8. P. Bas et al.,Geometrically InvariantWatermarking Using Feature Points,IEEE Trans. Image Processing, vol. 11, no. 9, 2002,pp. 10141028.
9. C.S. Lu et al., Denoising and Copy Attacks ResilientWatermarking byExploiting Prior Knowledge at Detector, IEEE Trans. Image Processing,vol. 11, no. 3, 2002, pp. 280292.
10. J. Barr et al., Using DigitalWatermarks with Image Signatures to Mitigatethe Threat of the Copy Attack, Proc. Intl Conf. Acoustics, Speech, andSignal Processing, IEEE Press, 2003, pp. 6972.
11. Q. Cheng et al., Robust Optimum Detection of Transform Domain Multiplicative Watermarks, IEEE Trans. Signal Processing, vol. 51, no. 4,2003, pp. 906924.
12. C.S. Lu aet al., Structural Digital Signature for Image Authentication: AnIncidental Distortion Resistant Scheme, IEEE Trans. Multimedia, vol. 5,no. 2, 2003, pp. 161173.
13. S. Craver et al., "Resolving Rightful Ownership with InvisibleWatermarking Techniques:Limitations, Attacks and Implications," IEEE J.Selected Areas in Comm., IEEE Press, 1998,pp. 573–586.
14. X.You et al., A Blind Watermarking Scheme Using New Nontensor Product Wavelet Filter Banks, IEEE Trans. Image Processing, vol. 19, no. 12,2010, pp. 32713284.