ISSN(Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Special Issue 6, May 2015

Uniform Embedding For Efficient Jpeg 2000 Steganography - Syndrome Trellis Coding

M.Suryadevi [1], S.Thenappan[2]

PG Student (Applied Electronics), Department of ECE Gnanamani College of Technology, Namakkal, India[1]

Assitant Professor, Department of ECE, Gnanamani College of Technology, Namakkal, India[2]

ABSTRACT: 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. The internet as a whole does not use secure links, thus information in transit may be vulnerable to interception as well. The important of reducing a chance of the information being detected during the transmission is being an issue now days. In this paper, we proposed a class of new distortion functions known as uniform embedding distortion function (UED) is presented. By incorporating the syndrome trellis coding, the best code word with undetectable data hiding is achieved. Due to hiding more amounts of data into the intersected area, embedding capacity is increased. Our aim is to hide the secret information behind the image file. In order to reduce the distortion between the cover object and stego object is an important issue for steganography. In this way statistically undetectable data can be increased.

KEYWORDS: Uniform Distortion Function;

I.INTRODUCTION

Steganography is an art and a science of communicating in a way, which hides the existence of the communication. It is also called as covered writing because it uses a cover of a message for sending any important secret message. Steganography serves as a means for private, secure and sometimes malicious communication. Steganography is the art to hide the very presence of communication by embedding the secret message into the innocuous-looking cover media objects.

Steganography is a powerful tool which increases security in data transferring and archiving. Steganography can be applied to different objects like text, picture, image, audio or video. This objects called cover object or carrier object of the steganographic method. The secret message can also be of types like text, picture, image, audio or video. These objects are called message object. After application of steganographic method the produced output file is called stego-object. Cryptography is an art of sending the secret information in the unreadable form. Both Steganography and Cryptography have the same goal of sending the secret message to the exact receiver.

In Steganography, the secret message is hidden in any of the cover medium and then transmitted to the receiver, whereas in cryptography, the secret message is made unreadable and then transmitted to the receiver in an unreadable form. The message that is sent to receiver through cryptography, express out that some secret communication is going on between the sender and the receiver. This leads to the main drawback of the cryptography. In steganography, only the sender and receiver know the secret communication. Image steganography is carried out using different techniques.

This method is broadly classified based on Spatial-domain and transform-domain. In Spatial domain, the secret messages are embedded directly. The steganography scheme embeds the secret message by modifying the Gabor coefficients of the cover image. The data hiding technique using DWT was performed on both the secret and cover images. The secret message is embedded in the high frequency coefficients in DWT performed on cover. This approach of information hiding technique has recently become important in a number of application areas. Digital audio, video, and pictures are increasingly furnished with distinguishing but imperceptible marks of existence. This project comprehends the following objectives:

ISSN(Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Special Issue 6, May 2015

To produce security tool based on steganographic techniques. To reduce the distortion between the cover object and stego object is an important issue for steganography.

II. EXISTING SYSTEM

Steganography is the science and art of Secret communication where the sender embeds secret message into an original image (cover) with a shared key to generate a stego image. To conceal the very existence of communication, the stego image has to be statistically undetectable from its cover counterpart. Therefore, the two conflicting objectives undetectability and embedding payload, should be carefully considered when devising a steganographic scheme. $\mathbf{x} \in R^n$ and $\mathbf{y} \in R^n$ as the cover and stego images, respectively. We then define the cost (or distortion) function of making an embedding change at i -th element of $\mathbf{x}$ from x_i to y_i as $\rho_i(x_i, y_i)$, where $0 \leq \rho_i < \infty$. Under the additive distortion model, the total impact caused by the embedding can be expressed as the sum of embedding cost over all elements, i.e., $D(\mathbf{x}, \mathbf{y}) = \_ni=1 \rho i (xi, yi)$. In practice, the problem of designing a secure steganographic scheme can be formulated as the minimal distortion embedding, i.e., to minimize the total embedding distortion D for a given payload. With properly designed ρ_i , the total statistical artifacts caused by the embedding are minimized and the resulting stego objects can be made less detectable. As JPEG is the most widely used format for digital image storage and transmission, JPEG steganography has become the domain of extensive research. It has witnessed the development of a lot of schemes for JPEG steganography over the last decade, such as F5 , nsF5, MME and some recently emerged adaptive ones. All of these schemes can be described with a unified framework, the minimal distortion embedding framework, which consists of the coding unit and the distortion function. In the F5, the embedding impact is treated equally for each coefficient. As a result, minimizing the total distortion f or a given payload corresponds to the effort to minimize the number of coefficients to be modified, or maximize the embedding efficiency, i.e., the number of message bits embedded per embedding change.

The security performance of F5 was improved by increasing its embedding efficiency through matrix encoding, which can be viewed as a special case of the minimal distortion embedding frame work with the embedding cost being identical for each coefficient. In, the wet paper code (WPC) is incorporated in nsF5,improved version of F5, to tackle the issue of shrinkage withF5, resulting in significant improvement in coding efficiency compared to the Hamming code used in F5. In the MME, for JPEG steganography, the advantage of the side-information of the original uncompressed image is taken to construct the distortion function, furthermore, only those coefficients with less distortion are selected to be modified, and more coefficients may be modified compared with the matrix coding proposed in another efficient JPEG steganographic scheme, denoted as BCH opt, based on heuristic optimization and fast BCH syndrome coding. Compared with the MME, the BCH opt takes into account not only the rounding error but also the quantization step in the construction of distortion function, thus leading to significant improvement in security performance against st performance gain of both MME and BCH opt stems largely from the original BMP image as pre cover, which is, however, not always available in practice.

In Filler proposed to use syndrome trellis coding (STC) as a practical approach for the implementation of minimal distortion embedding framework. They have shown that, under the additive distortion model, the STC can achieve asymptotically the theoretical bound of embedding efficiency for a user-defined distortion function.

III. EXISTING BLOCK DIAGRAM

Preprocessing: The pre-processing is adapted to generate the cover the quantized DCT coefficients for data embedding.
Case 1: When input image is original BMP image, the process starts from the implementation of JPEG compression. In this way, the side-information, i.e., the rounding error is Propo sed scheme. (a) Data embedding. (b) Data extraction. available for a more secure data embedding. Let $\mathbf{c}_ = _c_k_$and $\mathbf{c} = \{ck\}$ be the quantized DCT coefficients before andafter rounding operation, respectively. Then the rounding error is obtained with $rk = ck - c\_k$.
Case 2: When the input image is in JPEG format, theentropy decoding is applied to generate the quantized DCT coefficients $\mathbf{c}$ directly.In both cases, we obtain the scrambled non-zero AC coefficients$\mathbf{x}$ from $\mathbf{c}$ by a shared key K, i.e.,$\mathbf{x} = fnz(\mathbf{c},K) = \{xk\}$, (11)where $fnz()$ is the mapping function. Similarly $\mathbf{x}\_ = fnz\ \_\mathbf{x}\_,K\_ = \_x\_k\_$ denotes the scrambled non-zero AC coefficients before rounding.

ISSN(Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Special Issue 6, May 2015

2) Embedding Operation: Let **y** = {*yk* } and _ be the scrambled stego DCT coefficients and embedding operation,respectively. For scrambled AC coefficients **x** = {*xk*}, wehave *yk* = *xk* + _*k*. Before evaluating the distortion of a modified coefficient, the embedding operation _ itself should be defined.

Case 1: With the original BMP image, the embedding operation _ is defined as below,

$$\_k = \begin{cases} +1, \text{ if } rk \le 0 \ \& \ xk \_ = -1-1, \text{ if } rk \le 0 \ \& \ xk = -1-1, \text{ if } rk > 0 \ \& \ xk \_ = 1+1, \text{ if } rk > 0 \ \& \ xk = 1 \end{cases}$$

The embedding error due to data embedding is

$$r\_k = yk - x\_k$$

$$= xk + \_k - x\_k = \_k + rk = \begin{cases} 1 + rk \text{ , if } rk \le 0 \ \& \ xk \_ = -1-1 + rk \text{ , if } rk \le 0 \ \& \ xk = -1 \\ -1 + rk \text{ , if } rk > 0 \ \& \ xk \_ = 1 \\ 1 + rk \text{ , if } rk > 0 \ \& \ xk = 1 \end{cases}$$

$$|r\_k| = \begin{cases} 1 - |rk|, \text{ if } rk \le 0 \ \& \ xk \_ = -1 \\ 1 + |rk|, \text{ if } rk \le 0 \ \& \ xk = -1 \\ 1 - |rk|, \text{ if } rk > 0 \ \& \ xk \_ = 1 \\ 1 + |rk|, \text{ if } rk > 0 \ \& \ xk = 1 = \_1 + |rk|, \text{ if } xkrk > 0 \ \& \ |xk| = 1 \\ 1 - |rk|, \text{ otherwise} \end{cases}$$

Thus we have the resulting additional rounding error

$$ek = |r\_k| - |rk| = \begin{cases} \_1, \text{ if } xkrk > 0 \ \& \ |xk| = 1 \\ 1 - 2|rk|, \text{ otherwise} \end{cases}$$

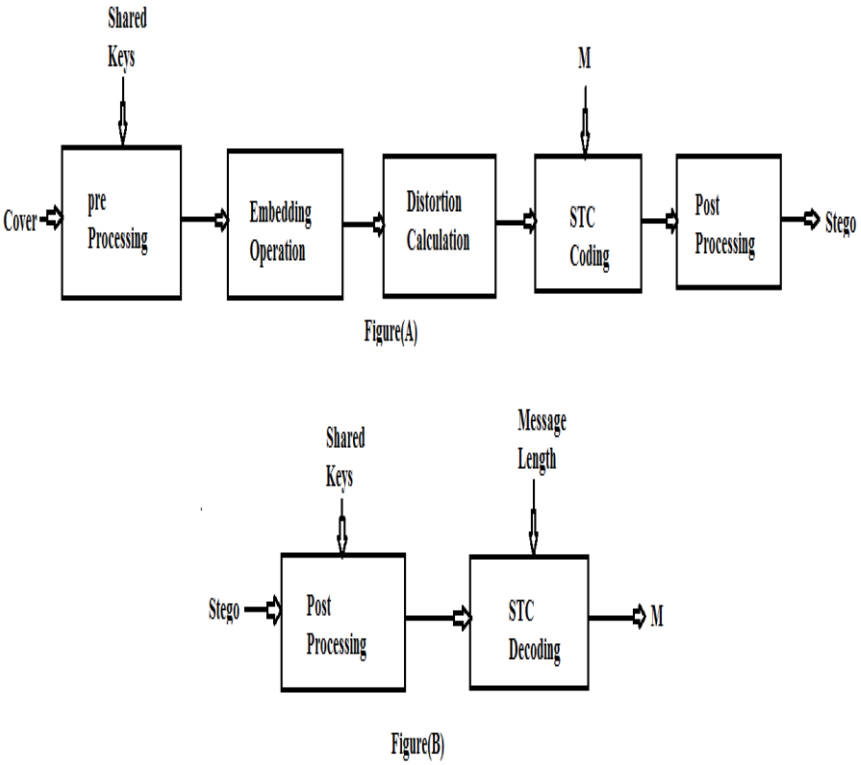

Figure 1 Existing Block Diagram

Case 2: When the side-informed original BMP image is notavailable, the embedding operation _ is simply defined as_*k* =_sgn*(xi)*, if |*xk*| = 1±1, if |*xk*| _= 1 In both cases, we increase the absolute value of those ±1 cover coefficients by 1 so that no additional zero DCT coefficients are created

ISSN(Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Special Issue 6, May 2015

3) Distortion Calculation:
Case 1: Compute the embedding distortion $\rho = \{\rho k\}$ for each scrambled non-zero AC coefficient x_k using the SI-UED defined in (10), where the additional rounding error is computed.
Case 2: Compute the embedding distortion $\rho = \{\rho k\}$ for each scrambled non-zero AC coefficient xk using the JC-UED

4) STC Coding:
Case 1: Since the embedding operation is deterministic as in (12) which is guided by the rounding error, we can only use the binary STC. Let the binary vector **m** = {*mi* } and **xb** = {*xbi* } be the secret message and LSB of cover **x**, respectively. With **m**, **xb** and its corresponding embedding cost ρ as input parameters, the binary STC coding [1] is then applied to embed secret message **m** to **x**. The output of STC is the stego **x_b** for **xb**, which is then used to construct the modified pattern **p** = xor*(***xb**, **x_b***)* of scrambled non-zeroAC coefficients **x**.
Case 2: Unlike case 1, the embedding operation is nondeterministic as in (15) except that $|xk| = 1$. Since embedding operation can randomly be +1 or −1, this allows us to use the ternary STC to further improve the security performance. With **m**, **x** and its corresponding embedding cost ρ as input parameters, the ternary STC coding [1] is then applied to embed secret message **m** to **x**. And the output of STC is directly the stego **y**.

5) Post processing:
Case 1: Once the modified pattern **p** = xor*(***xb**, **x_b***)* is obtained, the cover **x** is modified with (16)to obtain stego **y**. $\_k$ is defined in $yk = \_xk$, if $pk = 0$ $xk + \_k$, if $pk = 1$
For both cases, the entropy coding is then applied to generate stego JPEG image after **y** is descrambled.

B. Data Extraction
1) Preprocessing: For a stego JPEG image, the quantized DCT coefficients are obtained by entropy decoding, which are then scrambled with the shared key K to generate the scrambled non-zero AC coefficient **y**.
2) STC Decoding: The STC decoding (binary STC for Case 1 and ternary STC for Case 2) is then applied to extract the secret message **m**.

IV. PROPOSED SYSTEM

In this paper, we focus on the design of a new additive distortion function for JPEG steganography. By following the concept in spirit of spread spectrum communication", the proposed distortion function is designed so as to guide the stego system to uniformly spread the embedding modification to the quantized DCT coefficients of all possible magnitudes. This results in possible minimal artifacts of first- and second-order statistics for DCT coefficients as a whole. It is noted that, for non side-informed JPEG steganography, our proposed distortion function is derived directly from the quantized block DCT coefficients without any pre-model training. An efficient JPEG steganographic scheme is then developed by incorporating the new distortion function in the STC framework, which works quite well against the popular steganalyzers with various feature sets

This paper Proposed includes several new contributions:
1) The detailed analysis why the proposed UED function can lead to less average changes of second-order statistics besides the first-order ones;
2) The analysis of the allowable modification (embedding) rate of DCT coefficients with different magnitude from the perspective of natural image model;
3) The new scheme for side-informed JPEG 2000 steganography; and
4) Implementation of all the experiments on the new BOSS base image database, which is widely considered as a more appropriate benchmark to evaluate the performance of the steganographic and steganalytic schemes.

ISSN(Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Special Issue 6, May 2015

V. PROPOSED BLOCK DIAGRAM

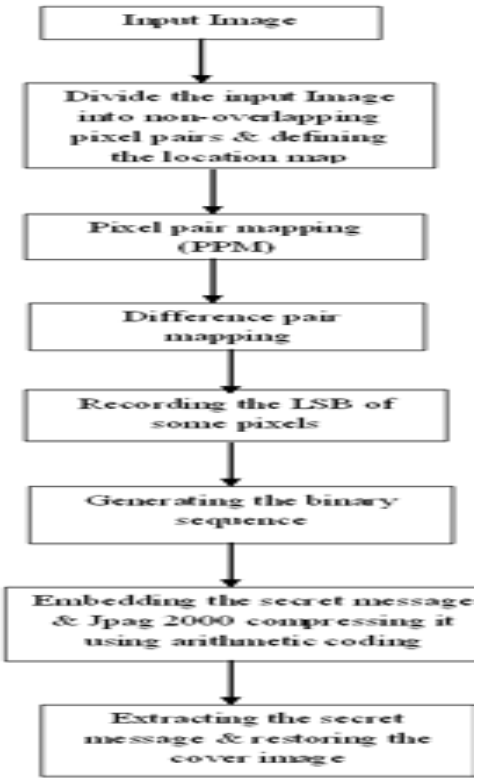

Figure 2 Proposed Block Diagram

VI DIGITAL WATERMARKING

A digital watermark is a kind of marker covertly embedded in a noise-tolerant signal such as audio or image data. It is typically used to identify ownership of the copyright of such signal. Watermarking is the process of hiding digital information in a carrier signal; the hidden information should, but does not need to contain a relation to the carrier signal. Digital watermarks may be used to verify the authenticity or integrity of the carrier signal or to show the identity of its owners. It is prominently used for tracing copyright infringements and for banknote authentication. Like traditional watermarks, digital watermarks are only perceptible under certain conditions, i.e. after using some algorithm, and imperceptible anytime else. If a digital watermark distorts the carrier signal in a way that it becomes perceivable, it is of no use. Traditional Watermarks may be applied to visible media (like images or video), whereas in digital watermarking, the signal may be audio, pictures, video, texts or 3D models. A signal may carry several different watermarks at the same time. Unlike metadata that is added to the carrier signal, a digital watermark does not change the size of the carrier signal.

The needed properties of a digital watermark depend on the use case in which it is applied. For marking media files with copyright information, a digital watermark has to be rather robust against modifications that can be applied to the carrier signal. Instead, if integrity has to be ensured, a fragile watermark would be applied. Both steganography and digital watermarking employ steganographic techniques to embed data covertly in noisy signals. But whereas steganography aims for imperceptibility to human senses, digital watermarking tries to control the robustness as top priority.
Since a digital copy of data is the same as the original, digital watermarking is a passive protection tool. It just marks data, but does not degrade it non-controls access to the data. One application of digital watermarking is source tracking.

ISSN(Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Special Issue 6, May 2015

A watermark is embedded into a digital signal at each point of distribution. If a copy of the work is found later, then the watermark may be retrieved from the copy and the source of the distribution is known. This technique reportedly has been used to detect the source of illegally copied movies.

VII APPLICATIONS

Digital watermarking may be used for a wide range of applications, such as:

- Copyright protection
- Source tracking (different recipients get differently watermarked content)
- Broadcast monitoring (television news often contains watermarked video from international agencies)

DIGITAL WATERMARKING LIFE-CYCLE PHASES

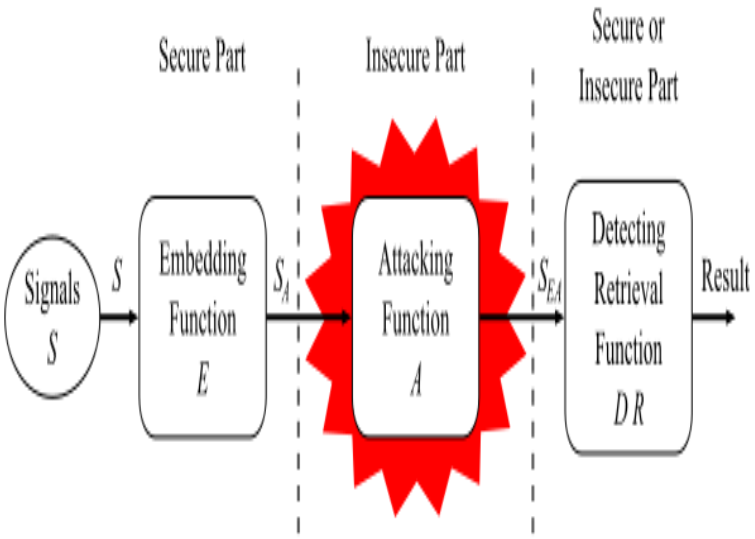

Figure 3 Proposed Block Diagram

General digital watermark life-cycle phases with embedding-, attacking-, and detection and retrieval functions. The information to be embedded in a signal is called a digital watermark, although in some contexts the phrase digital watermark means the difference between the watermarked signal and the cover signal. The signal where the watermark is to be embedded is called the host signal.

IX. CLASSIFICATION

A digital watermark is called robust with respect to transformations if the embedded information may be detected reliably from the marked signal, even if degraded by any number of transformations. Typical image degradations are JPEG compression, rotation, cropping, additive noise, and quantization. For video content, temporal modifications and MPEG compression often are added to this list. A digital watermark is called imperceptible if the watermarked content is perceptually equivalent to the original, un watermarked content. In general, it is easy to create robust watermark or imperceptible watermarks, but the creation of robust imperceptible watermarks has proven to be quite challenging. Robust imperceptible watermarks have been proposed as tool for the protection of digital content.

A watermarking system is usually divided into three distinct steps, embedding, attack, and detection. In embedding, an algorithm accepts the host and the data to be embedded, and produces a watermarked signal. Then the watermarked digital signal is transmitted or stored, usually transmitted to another person. If this person makes a modification, this is called an attack. While the modification may not be malicious, the term attack arises from copyright protection application, where third parties may attempt to remove the digital watermark through modification. There are many

ISSN(Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Special Issue 6, May 2015

possible modifications, for example, lossy compression of the data (in which resolution is diminished), cropping an image or video, or intentionally adding noise.

Detection (often called extraction) is an algorithm which is applied to the attacked signal to attempt to extract the watermark from it. If the signal was unmodified during transmission, then the watermark still is present and it may be extracted. In robust digital watermarking applications, the extraction algorithm should be able to produce the watermark correctly, even if the modifications were strong. In fragile digital watermarking, the extraction algorithm should fail if any change is made to the signal.

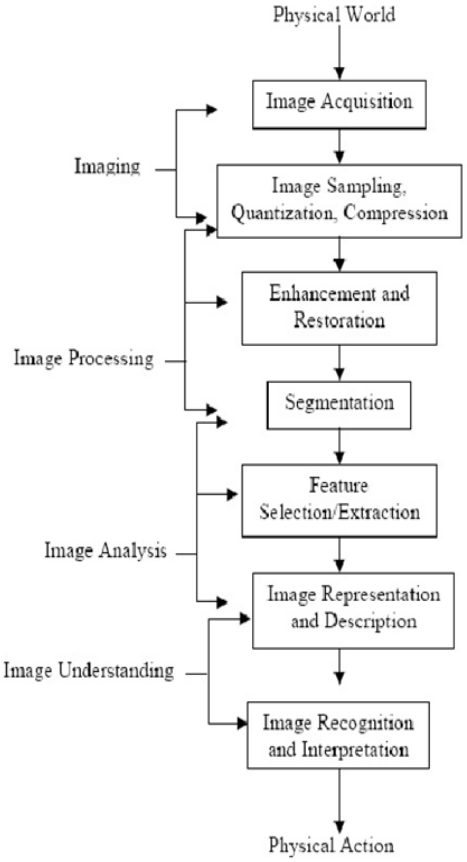

Figure 4 Important steps involved in digital image processing Water marking

X. CONCLUSION

Minimal-distortion embedding framework is a practical approach to implement JPEG steganography with high embedding efficiency. In this paper, an efficient JPEG steganographic scheme which utilizes syndrome trellis coding (STC) and uniform embedding (UE) strategy is presented. The uniform embedding is similar in spirit to spread spectrum communication. By uniformly spreading the embedding modifications to quantized DCT coefficients of all possible magnitudes, the average changes of first- and second-order statistics are possibly minimized, especially in the small coefficients,which leads to less statistical detectability, and hence, more secure steganography. A class of new distortion functions known
as uniform embedding distortion function (UED) for both non side-informed and side-informed JPEG steganography are developed to incorporate the uniform embedding. The JC-UED for non side-informed embedding takes into account

ISSN(Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Special Issue 6, May 2015

the magnitude of DCT coefficient as well as both According to some of our experiments, some DC and zero AC coefficients in the texture regions could indeed be incorporated to further data embedding without decreasing, even increasing the security performance. While the UED proposed in this paper could by no means tackle all of these issues, it raises a quite challenging open question, that is how to evaluate the embedding costs of all possible DCT coefficients (including DCs, zero and nonzero ACs) based solely on the coefficients in the DCT domain for JPEG steganography, which remains as the topic of our future research effort to use JPEG 2000 by we gave a Compressed Image and a Image Quality will be Increased.

REFERENCES

[1] T.Filler, J. Judas, and J. Fridrich, "Minimizing additive distortion in steganography using syndrome-trellis codes," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 3, pp. 920–935, Sep. 2011.
[2] A. Westfeld,"F5—A steganographic algorithm," in *Proc. 4th Inf. Hiding Conf.*, vol. 2137. 2001, pp. 289–302.
[3] J. Fridrich, T. Pevný, and J. Kodovský, "Statistically undetectable JPEG steganography: Dead ends challenges, and opportunities," in *Proc. 9th ACM Workshop Multimedia Security*, Dallas, TX, USA, Sep. 2007,
[4] Y. Kim, Z. Duric, and D. Richards, "Modified matrix encoding technique for minimal distortion steganography," in *Proc. 8th Inf. Hiding Conf.*, vol. 4437. Jul. 2006, pp. 314–327.
[5] V.Sachnev, H. J. Kim, and R. Zhang, "Less detectable JPEG steganography method based on heuristic optimization and BCH syndrome coding," in *Proc. 11th ACM Workshop Multimedia Security*, Sep. 2009
[6] T.Filler and J. Fridrich, "Design of adaptive steganographic schemes for digital images," *Proc. SPIE*, vol. 7880, p. 78800F, Jan. 2011.
[7] C. Wang and J. Ni, "An efficient JPEG steganographic scheme based on the block entropy of DCT coefficients," in *Proc. IEEE ICASSP*, Kyoto, Japan, Mar. 2012, pp. 1785–1788.
[8] J. Kodovský and J. Fridrich, "Calibration revisited," in *Proc. 11th ACM Workshop Multimedia Security*, New York, NY, USA, Sep. 2009,
[9] J. Kodovský, J. Fridrich, and V. Holub, "On dangers of overtraining steganography to incomplete cover model," in *Proc. 13th ACM Workshop Multimedia Security*, New York, NY, USA, Sep. 2011,
[10] V. Holub and J. Fridrich, "Digital image steganography using universal distortion," in *Proc. 1st ACM Workshop Inf. Hiding Multimedia Security*,2013, pp. 59–68.
[11] J. Kodovský and J. Fridrich, "Steganalysis of JPEG images using rich models,"*Proc. SPIE*, vol. 8303, p. 83030A, Jan. 2012.
[12]J. Kodovský, J. Fridrich, and V. Holub, "Ensemble classifiers for steganalysis of digital media," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 2, pp. 432–444, Apr. 2012.
[13] C.Chen and Y. Q. Shi, "JPEG image steganalysis utilizing both intrablock and interblock correlations," in *Proc. IEEE Int. Symp. Circuits Syst.*, Mar. 2008, pp. 3029–3032.
[14] L. Guo, J. Ni, and Y. Q. Shi, "An efficient JPEG steganographic scheme using uniform embedding," in *Proc. 4th IEEE Int. Workshop Inf. Forensics Security*, Tenerife, Spain, Dec. 2012, pp. 169–174.
[15] P. Bas, T. Filler, and T. Pevný, "Break our steganographic system—The ins and outs of organizing boss," in *Proc. 13th Inf. Hiding Conf.*, 2011,pp. 59–70.
[16] N. Provos, "Defending against statistical steganalysis," in *Proc.10th USENIX Security Symp.*, Washington, DC, USA, 2001,
[17] D. Freedman, *Statistical Models: Theory and Practice*. Cambridge, U.K.: Cambridge Univ. Press, 2009.
[18] C.-C. Chang and C.-J. Lin, "LIBSVM: A library for support vector machines," *ACM Trans. Intell. Syst. Technol.*, vol. 2, no. 3