Websites:
http://www.sciencepub.net/newyork
http://www.sciencepub.net

Emails:
newyorksci@gmail.com
editor@sciencepub.net

New York Science Journal

MARSLAND PRESS
Multidisciplinary Academic Journal Publisher

A Novel Approach for Compressing Welding Radiographic Images Using Multilevel Steganography

Dr.V.Vaithiyanathan[1], B. Karthikeyan[1], Anishin Raj M M[1], Dr.B.Venkatraman[2]

[1] School of Computing, SASTRA University, Thanjavur-613401, India
[2] Associate Director, RSEG, Indira Gandhi Center for Atomic Research, Kalpakkam-603102, India
mbalakarthi@gmail.com

Abstract: Steganography is the art of concealing data within data in such a way that it is almost untraceable. Out of the multitude of information carriers, digital images are the most popular ones used in steganography. Various techniques of concealing information exist for various kinds of applications. Every application calls for different requirements and appropriate techniques have to be chosen accordingly. Steganography contributes vastly to the field of security and helps to lessen foul play or breach of information sharing rules. Embedding a small amount of pixel information of an original image into a larger image where each of its pixels contains information related to the original image makes it almost difficult to retrieve the actual information. The reverse process points towards the decompression of the larger image until the original information is found. This type of process uses LSB technique of pixel embedding and is widely used for a variety of applications. It serves the dual purpose of securing vital information by obscuring it in addition to compressing the image information for resourceful use of memory.

[Vaithiyanathan V, Karthikeyan B, M M Anishin Raj, Venkatraman B. **A Novel Approach for Compressing Welding Radiographic Images Using Multilevel Steganography**. *N Y Sci J* 2021;14(8):8-13] ISSN 1554-0200 (print); ISSN 2375-723X (online) http://www.sciencepub.net/newyork.2. doi:10.7537/marsnys140821.02.

Keywords: Steganography, Compression, LSB Substitution, Weld defect

1. Introduction

With the advent of Internet, steganography has evolved into a major subject of interest in the field of information security. Any digital file formats that act as information carriers can be used for steganography. The files must possess a high degree of redundancy to provide unparalleled accuracy. This feature also lays focus on compression of files. These digital files or information carriers can be of various forms including texts, images, audios, videos and other protocols. But, digital images comply with the redundancy requirements and are most suitable for compression as well as steganography by pixel data embedding. Steganography can be applied to various scenarios including medical imaging, remote sensing, images with legal information and valuable arts protection.

A good steganography scheme is judged by the imperceptibility, capacity and robustness of the embedded information. The resulting image must be so similar to the original one which turns into an almost impossible task. Robustness of a steganographic scheme is determined by speed and amount of information embedded [7-10]. Robustness to familiar attacks involve low pass filtering, frame dropping, transcoding and noisy interface in addition to robustness to compression techniques must be kept in check. After pixel embedding, the image should be such that infiltration of critical data is unfeasible. In such a case, the attacker is likely to fail in his efforts to conclude authenticity of original information.

Digital images are numerically portrayed as a grid of diminutive points known as pixels. The pixels are represented in bits [2-3]. Bit depth gives the measure of bits composed in each pixel of a color scheme. Bit depths can vary from 1bit for a monochrome image to 64 bits for a deep color image [4-6]. Typically digital images are represented as 24 bits with each byte pertaining to the three primary colors of the RGB model.

Larger images tend to have large bit depths posing a hindrance for convenient data transmission. Hence, images have to be condensed to relieve both spatial and time complexities. The compression process can be carried out in two methods viz. lossy compression and lossless compression [15]. Lossy compression produces close approximation of original image, although it's not the exact replica, while lossless compression maintains the integrity of the original image. As the concept of lossy compression is fundamentally at par with information hiding, it is essential to find a suitable tradeoff between crucial data hiding requirements, imperceptibility, capacity and robustness prior to compression. This detains the perceptual compression algorithm from purging superfluous information related to the embedded data [16-18].

2. Proposed Methodology

The proposed methodology consists of embedding and extracting phase which are being depicted below in the Figure 1 and Figure 2.

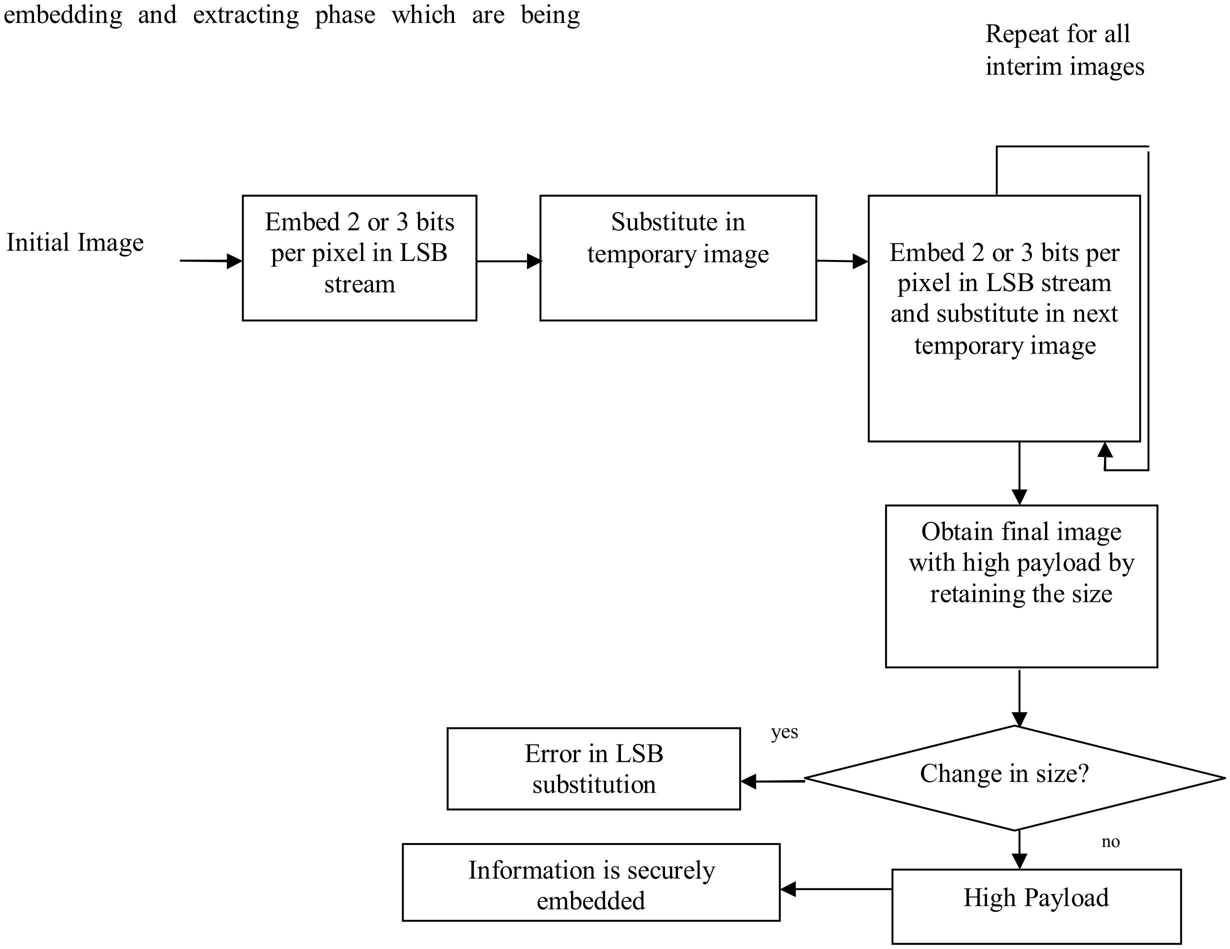

Repeat for all interim images
Initial Image
Embed 2 or 3 bits per pixel in LSB stream
Substitute in temporary image
Embed 2 or 3 bits per pixel in LSB stream and substitute in next temporary image
Obtain final image with high payload by retaining the size
Change in size?
yes
Error in LSB substitution
no
High Payload
Information is securely embedded

Figure 1.Embedding phase for the image incorporation

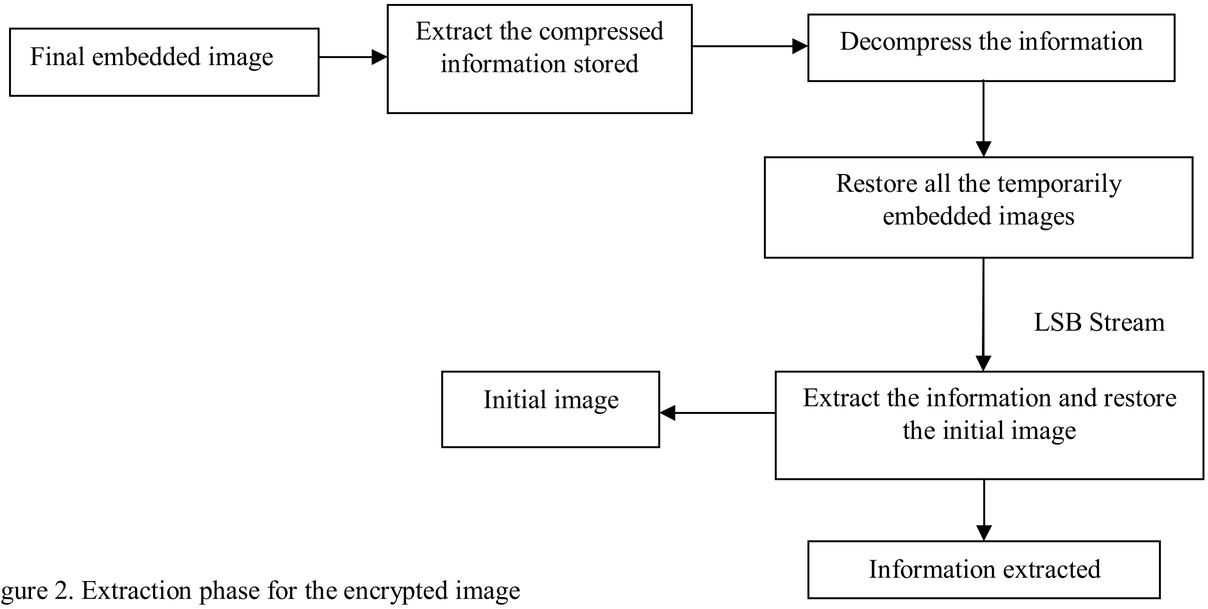

Final embedded image
Extract the compressed information stored
Decompress the information
Restore all the temporarily embedded images
LSB Stream
Extract the information and restore the initial image
Initial image
Information extracted

Figure 2. Extraction phase for the encrypted image

Table 1. Performance Evaluation for embedding phase

Result	Input	Dimension	Size (KB)	MSE		
				R	**G**	**B**
R 1	Input 1	50 x 50	8	0	0	0
	Input 2	100 x 100	30	2.4224	2.4527	2.4506
	Input 3	227 x 355	238	1.2339	1.2229	1.2256
	Input 4	1567 x 804	3694	0.7295	0.729	0.7293
R 2	Input 1	16 x 16	1	0	0	0
	Input 2	64 x 64	13	0.6389	0.5901	0.5637
	Input 3	128 x 128	49	1.9521	1.9282	2.1833
	Input 4	256 x 256	193	2.3986	2.4832	2.4177
	Input 5	512 x 512	769	2.2249	2.3464	2.2448
	Input 6	1024 x 1024	3073	2.4114	2.3764	2.7314
R 3	Input 1	40 x 30	2	0	0	0
	Input 2	100 x 101	30	1.6595	1.6649	1.6805
	Input 3	352 x 288	298	1.2641	1.2708	1.2.84
	Input 4	717 x 717	1507	1.975	1.9541	1.9764
	Input 5	1434 x 1434	6028	2.5837	2.6167	2.5228
R 4	Input 1	64 x 64	13	0	0	0
	Input 2	158 x 130	61	1.8192	1.9302	1.8417
	Input 3	512 x 512	769	0.7154	0.6998	0.7228
	Input 4	1024 x 1024	3073	2.3504	2.6082	2.3609

3.Experimental Results and Discussion

The Least significant bit (LSB) substitution method is popularly used to embed message data within an image [1]. Commonly LSBs of an image are assumed to be the ideal positions to embed information as they not only yield minimal perceptible quality loss but are also significantly random in nature. The LSB substitution method follows the concept of modifying each pixel value and covering its visibility without hampering the potential changes. This shifts focus on a vast quantity of redundancy in the pixel information. Thus, the LSBs of the image data can be effectively replaced with each bit of the message data. This process can be continued until the whole message has been embedded [22].

Four sample gray scale images of dissimilar dimensions, each larger than the preceding one, are considered for trialing. Each pixel comprises of 24bits with 8 bits owed to each of the color dimensions, red, blue and green. Last 3 LSBs are given due consideration for substitution. The number of bits to replace can be decided as per requirements. Ideally 2 or 3 bits per color is chosen. The amount of information stored gradually increases with the increase in number of bits substituted. In this case, 3 bits each in each of the color dimensions are chosen summing up to 9 bits in the whole. The amount of information of the initial image embedded in each pixel of the succeeding image is given by the equation.

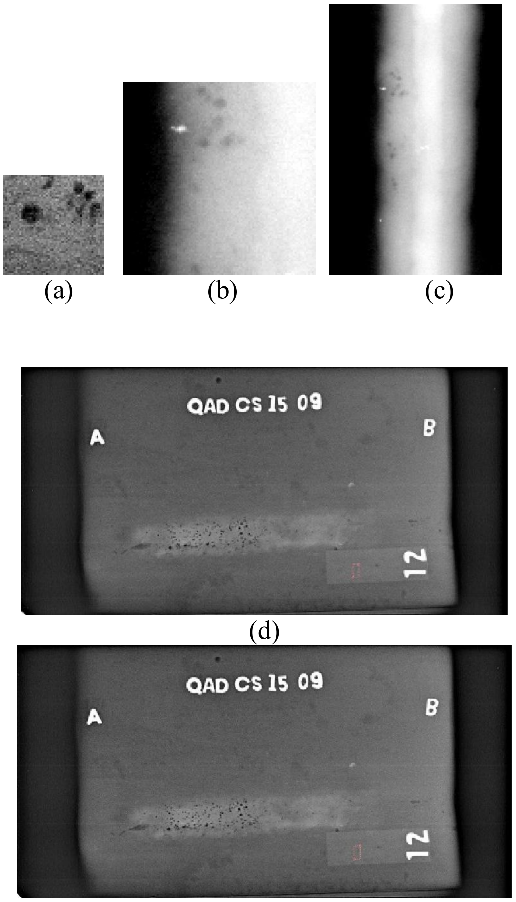
$$I = \frac{S \times N}{L}$$

Where, I is the information embedded, S is the size of the image, N represents the number of bits in each pixel, 24 in this case and L corresponds to the number of LSBs substituted in each pixel.

The concept of substituting or replacing the pixel information does not compromise with the consumption of space [11-12]. The sizes of the images remain unaltered although the image contains ample additional information crucial to the preceding images.

The embedding phase is described in the flow chart mentioned in the proposed methodology on the initial cover image and the procedure is carried out iteratively on the succeeding images as well. The final image encompasses all the vital information of all the preceding images. The resultant images are shown in Figure 3.

Successively, the extraction phase is carried out as a result of which the entire pixel information can be effectively decoded. The resultant images after each iterative step are represented in Figure 4. The final image obtained is the original cover image.

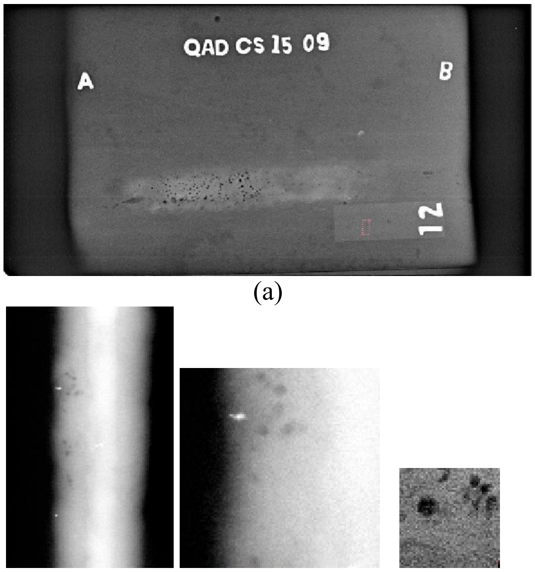


(a) (b) (c)

(d)

(e)

Figure 3. Gray Scale samples of RGB images during embedding phase. (a) Sample cover image (b) Stego image embedded with information of cover image,(c) Multiple image information embedding the cover and initial stego image (d) Compressed high payload embedded image,(e) Final Stego Image



(a)

(b) (c) (d)

Figure 4: Gray Scale samples of RGB images during extraction phase. (a) Stego image (b) Image decoded from final stego image.(c) Multiple image information decoded from intermediate stego image containing information of cover and initial stego image (d) Initial cover image.

Invariability of size despite high payload is the essence of the experiment. It ensures information confidentiality and increases security. Hence, the extraction phase is more strenuous in comparison to the embedding phase. The original data can be procured by the developer/embedder but a third party intervention is unlikely [13-14].

The performance of whole process can be evaluated using Mean Squared Error as depicted in the table below [23]. The MSE values vary as per the number, size and type of image. It is evident from the table that the initial image has no pre conditions to be compared to which makes its MSE values zero across all the three dimensions. The rest of the images have additional information, which gradually increase with the number of images in a single phase of embedding. The results can be tested on multiple images with different types and sizes (Table 1). MSE is expected to be minimal for the stego image to be robust and undecipherable. Higher error values make the information vulnerable [19-21].

4. Conclusion

The experiment carried out on the sample images unraveled many aspects of pixel embedding and highlighted its significance in terms of data protection. Multiple trials using various images infer that images with minimal MSE are most protected, R1 in this case. However, the complexity of the process increases with the number of pixels embedded, demanding more sophisticated ways of embedding. Developments in steganography can open up new horizons in the field of information hiding, image compression, signal frequency modulation, copyright protection and peer to peer communication.

Acknowledgement:

The authors would like to express their sincere thanks to Indira Gandhi Center for Atomic Research (IGCAR), Kalpakkam, Tamil Nadu, India, for providing the radiographic weld images for this research work.

Corresponding Author:
B. Karthikeyan, Assistant Professor,
Department of IT
School of Computing
SASTRA University,
Thanjavur-613401, India

References

[1]. Qingzhong Liu, Andrew H. Sung, Bernardete Ribeiro, Mingzhen Wei, Zhongxue Chen, Jianyun Xu, Image complexity and feature mining for steganalysis of least significant bit matching steganography, Information Sciences 2008;178: 21–36.

[2]. Mei-Yi Wu, Yu-Kun Ho, Jia-Hong Lee, An iterative method of palette-based image steganography, Pattern Recognition Letters 2004; 25 : 301–309.

[3]. Abbas Cheddad, JoanCondell, KevinCurran, PaulMcKevitt, Digital image steganography: Survey and analysis of current methods, Signal Processing2010; 90: 727–752.

[4]. Tao Zhang a, Wenxiang Li, Yan Zhang, Ergong Zheng, Xijian Ping, Steganalysis of LSB matching based on statistical modeling of pixel difference distributions, Information Sciences 2010; 180 :4685–4694.

[5]. Vajiheh Sabeti, Shadrokh Samavi, Mojtaba Mahdavi, Shahram Shirani, Steganalysis and payload estimation of embedding in pixel differences using neural networks, Pattern Recognition 2010; 43: 405 – 415.

[6]. Nan-I Wu, Kuo-Chen Wu, Chung-Ming Wang, Exploring pixel-value differencing and base decomposition for low distortion data embedding, Applied Soft Computing 2012;12 : 942–960.

[7]. Chiang-Lung Liu, Shiang-Rong Liao, High-performance JPEG steganography using complementary embedding strategy, Pattern Recognition 2008; 41: 2945 – 2955.

[8]. Rengarajan Amirtharajan, John Bosco Balaguru Rayappan, An intelligent chaotic embedding approach to enhance stego-image quality, Information Sciences 2012; 193:115–124.

[9]. Chin-Chen Chang, The Duc Kieu, A reversible data hiding scheme using complementary embedding strategy, Information Sciences 2010; 180: 3045–3058.

[10]. Ju-Yuan Hsia, Ke-Fan Chan, J. Morris Chang, Block-based reversible data embedding, Signal Processing 2009; 89:556–569.

[11]. Xiaofeng Zhu, Zi Huang, Yang Yang, Heng Tao Shen, Changsheng Xu, Jiebo Luo, Self-taught dimensionality reduction on the high-dimensional small-sized data, Pattern Recognition 2013; 46:215–229.

[12]. Rafiullah Chamlawi, Asifullah Khan,Digital image authentication and recovery: Employing integer transform based information embedding and extraction, Information Sciences 2010; 180: 4909–4928.

[13]. Chang-Chou Lin, Wen-Hsiang Tsai,Secret image sharing with steganography and authentication, The Journal of Systems and Software 2004; 73:405–414.

[14]. Chin-Chen Chang, Wen-Chuan Wu, Yi-Hui Chen, Joint coding and embedding techniques for multimedia images, Information Sciences 2008; 178: 3543–3556.

[15]. Chin-Chen Changa, The Duc Kieu,Wen-Chuan Wu, A lossless data embedding technique by joint neighboring coding, Pattern Recognition 2009; 42: 1597 – 1603.

[16]. Li Fan, Tiegang Gao, Qunting Yang, Yanjun Cao, An extended matrix encoding algorithm for steganography of high embedding efficiency, Computers and Electrical Engineering 2011;37 :973–981.

[17]. Wien Hong, Tung-Shou Chen, Chih-Wei Luo, Data embedding using pixel value differencing and diamond encoding with multiple-base notational system, The Journal of Systems and Software 2012; 85:1166–1175.

[18]. C.L. Philip Chen, Mei-Ching Chen, Sos Agaian, Yicong Zhou, Anuradha Roy, Benjamin M. Rodriguez, A pattern recognition system for JPEG steganography detection, Optics Communications 2012; 285: 4252–4261.

[19]. S. Voloshynovskiy,O. Koval, F. Deguillaume, T. Pun, Quality enhancement of printed and scanned images using distributed coding, Signal Processing 2007; 87:1301–1313.

[20]. Wen-Jan Chen, Chin-Chen Chang, T. Hoang Ngan Le, High payload steganography mechanism using hybrid edge detector, Expert Systems with Applications 2010; 37:3292–3301.

[21]. Xian-ting Zenga, Zhuo Lib, Ling-di Pingb, Reversible data hiding scheme using reference pixel and multi-layer embedding, Int. J. Electron. Commun.(AEÜ) 2012; 66 : 532–539.

[22]. Hengfu Yang, Xingming Sun, Guang Sun, A High-Capacity Image Data Hiding Scheme Using Adaptive LSB Substitution, RADIOENGINEERING 2009; 18(4): 509-516.

[23]. Mehdi Kharrazi, Husrev T. Sencar, Nasir Memon, Performance study of common image steganography and steganalysis techniques, Journal of Electronic Imaging 2006, 15(4): 041104-1 - 041104-16.

3/2/2021