AN EFFICIENT ALGORITHMIC SOLUTION FOR HIGH PAYLOAD GOOD IMPERCEPTIBILITY HYBRID IMAGE STEGANOGRAPHY

A. Murtaza, F. Shaukat*, G. Raja and A.K. Khan

Department of Electrical Engineering, University of Engineering and Technology, Taxila, Pakistan.
Corresponding author's email: furqan.shoukat@uettaxila.edu.pk

ABSTRACT: A hybrid steganographic technique has been proposed to enlarge the size of secret message and to hide several images in one cover image. Initially, the secret images were compressed using JPEG 2000 before embedding them to the cover image. Second least significant bit plane of cover image was entirely replaced by secret message while tri-ways-pixel-value-differencing (TPVD) was used to hide secret message in remaining seven-bit cover image. The quality of stego image was enhanced by residual image coding (RIC). The cover image was divided in four sub-images, three of them provided cover for secret message using proposed technique while fourth sub-image was used to embed RIC of stego image using only TPVD, to ensure better quality in terms of peak signal to noise ratio (PSNR). Proposed technique provided the opportunity to transmit secret data without detection by different steganalysis techniques like dual statistics steganalysis. Experimental results verified that proposed technique achieved high payload with better image quality than TPVD scheme.

Keywords: Least significant bit replacement, Image hiding, Pixel-value differencing, Steganography, Data hiding.

(Received 03-12-2016 Accepted 11-06-2017)

INTRODUCTION

In digital communication, the need to protect secret data from being changed or stolen has been met with two solutions. One is cryptography which aims to make message unintelligible for those who are not target receivers. Only the target receiver with right key can decode the secret message. On the other hand steganography hides the message in a cover in such a way that existence of message is denied (Das *et al*., 2015 and Shen *et al*., 2015).

Progress in digital communication has entirely changed our life style. Today excessive use of digital images on social networks and on other applications of digital communication provides the opportunity to use digital images in watermarking or in steganography as a cover for hiding secret messages. A digital image carrying secret message is called stego-image. Opposed to water-marking which is used for copyright protection or authentication, steganography is used for secret communication (Sadek *et al*., 2015 and Adams, 2013) and the benchmarks are needed for steganography for capacity (payload calculated in terms of number of bytes of hidden message) and imperceptibility i.e quality of image measured in terms of peak signal to noise ratio reported by (Hsieh *et al.*, 2008).

Least significant-bits (LSB) replacement is one of the oldest and well known technique used for image steganography (Das *et al*., 2015). In LSB replacement method secret data is converted to single bit-stream which is used to replace fixed length LSB of each pixel in a cover image. This technique is prone to different steganalysis techniques which are used to detect presence of any secret message in a digital image. Achieving high payload and image quality simultaneously, is a difficult task in image steganography. However, there are some techniques based on pixel-value differencing (PVD) reported by (Gulve and Joshi, 2015) which provides both outstanding stego image quality and high payload successfully. In PVD, only one directional edge was used. Tri-way pixel-value differencing (TPVD) is improved version of PVD which uses three directional edges. Thus it provides higher payload capacity while maintaining acceptable stego image quality. In contrast to LSB, dual statistics steganalysis cannot detect presence of secret data embedded by TPVD or PVD reported by (Chang *et al*., 2008 and Wu *et al*., 2005).

To use digital images on internet and on many other applications their size must be reduced using one of compression standard like JPEG. One of them is JPEG 2000 (Sanjith *et al*., 2015 and Adams, 2013). The quality of secret images reduces due to JPEG2000 compression (Fig-1). Pointed out by Lee *et al*. (2012) who proposed a residual value coding based approach to compensate the quality reduction of the secret image (Figure-2).

In the proposed scheme, same concept has been used to compensate the quality of stego image. Steganographic technique proposed in this study uses 2nd bit plane substitution by secret message and then TPVD embedding over remaining 7-bit image to increase payload. Thus, the quality of stego image becomes special concern so one sub-image (partition of cover image) out of four sub-images is used only to embed RIC

of other three sub-images using only TPVD to maintain the quality of the stego image.

MATERIALS AND METHODS

High payload and high image quality of the secret images and for the stego image was the target of proposed steganographic scheme. The image quality was calculated by the resemblance of the processed image to the original image. Hence, PSNR was adapted to measure image quality. The quality of secret images reduced due to the process of compression for the purpose of minimizing the size of secret data to be embedded. While for stego image the process of steganography was the cause of reduction of its quality (Voloshynovskiy *et al*., 2001).

In the proposed method, secret images concatenated with their RIC were used as a message in the form of a single bit-stream. This bit-stream was implanted in the cover using 2nd bit plane replacement and TPVD on remaining 7-bit cover image, to produce stego image. To this end, residual value coding was applied to the stego image to enhance its quality (Lee *et al*., 2012).

Partition of cover image (Pre-procedure): The cover image was divided in four sub-images (Fig-3). Three sub-images were used in proposed multilevel steganographic scheme as a cover image to hide secret message which included secret images and their RIC. These sub-images were partitioned in non-overlapping 2x2 pixel blocks. Second bit of all pixels of under-processed block was replaced with bits from secret message. Pixels composed of remaining 7 bits were used to embed data by TPVD method. The 2nd bit was added back to achieve 8 bit pixels of stego image. The fourth sub-image (stego cover) was used to provide the cover for RIC of other three sub-images (stego images). In the fourth sub-image data embedding process used only TPVD (Chang *et al*., 2008).

Embedding Algorithm: Part (a) of Fig-4 shows the block diagram of proposed data embedding process. Initially, the original secret image was compressed using JPEG2000 compression standard (Adams, 2013 and Haiying *et al*., 2008) then RIC was acquired by performing residual image coding on the residual image obtained by subtracting actual secret image and pre-decompressed image. Next, entire secret message was obtained in the form of a long bit-stream by joining the RIC, RV and JPEG2000 compressed code of secret image. Both 2nd LSB replacement (Fridrich *et al*., 2001) and TPVD method were used on the three sub-images obtained by the partition of original cover to hide secret data. To this end, compensation by residual value coding was used for message cover to achieve better quality of stego image and RIC for message cover was obtained by residual image coding and embedded in fourth sub-image using TPVD. Finally, the stego image was generated by rejoining message cover and stego cover.

Extraction Algorithm: Part (b) of Fig-4 show the block diagram of proposed data extraction process. First, image cover and stego cover were separated from stego image. Then, hidden RIC for message cover was extracted from stego cover using TPVD extraction and the quantized residual image was subtracted from message cover to obtain low quality message cover. After this, secret message bit-stream was extracted from message cover using both LSB and TPVD extraction. Next, RIC of secret images was separated from JPEG2000 compressed code-stream of images. Finally, quantized residual image retrieved from RIC was added to the decompressed secret images.

RESULTS AND DISCUSSION

To experimentally verify the performance of proposed technique, 512X512 pixel gray-scale test images were used in different combinations of cover and secret images. Proposed scheme delivered better payload along with better PSNR for stego images. To compare performance of proposed scheme, secret images with same PSNR and size as were used by Lee *et al*. (2012) to analyze the PSNR of stego images for different amount of payload used.

Imperceptibility performance of the stego-image: Five different secret images were embedded in four different cover images to evaluate stego image quality. The minimum PSNR required for acceptable stego image quality was 38 dB as described by Voloshynovskiy *et al*. (2001). The different values of designed range table for TPVD were $w_k \in \{8,8,16,32,64,128\}$. The dimensions of used secret images and cover images were 512X512, except for the big image used as a secret image whose dimensions were 1024X1024. Fig. 5, 6 and 7, which showed the quality of the stego-image. The PSNR values were 42.52 dB, 44.02 dB and 41.90 dB. The size of big image was larger than the size of other four images, thus the PSNR was lower for the stego images acquired by hiding big image (Table-1).

The Imperceptibility performance of stego images obtained by using proposed scheme satisfied the minimum requirement of imperceptibility benchmark and was better than the performance of Lee's Technique (Fig-3). The proposed scheme was superior for hiding secret images which were larger than the cover images.

Payload evaluation: The maximum payload was defined by the capacity in terms of number of bytes that could be embedded to a given cover image. The transmission of larger secret messages was only possible by achieving higher payload. Higher payload provided the opportunity

to add redundancy to the secret message to achieve a more robust steganographic scheme.

Four different cover images of size $512X512$ were used. Table-2 shows the maximum achievable capacity of the cover images and respective value of PSNR for the proposed scheme and TPVD. It was noticeable that both the imperceptibility and payload achieved was better for the proposed scheme and all stego images satisfied the minimum imperceptibility benchmark.

Security verification using RS steganalysis: Steganalysis techniques were developed as the anti-steganography techniques to detect the presence of hidden data in an image. Dual statistics steganalysis developed by Fridrich *et al*. (2001) can successfully detect presence of hidden data by LSB substitution. In this method, the test image was partitioned in consecutive or disjoint groups of n pixels.

A discrimination function and flipping function represented by f and F respectively were used to separate three types of pixel groups based on regularity and smoothness. Three types of groups were Singular groups, Regular groups and Unusable groups. The amounts of Singular and Regular groups were calculated for the entire test image. The diagrams in which image pixels are drawn against the numbers of related Singular and Regular groups are called RS-diagrams. Fridrich *et al.* (2001) provided a quadratic equation to predict secret message length p based on the curves of RS-diagram. A negative value of p means there is no hidden message in the test image. Maximum value of p is 100%. Table 3 shows the experimental results of the security verification by RS-steganalysis for different cover images, which were embedded with different secret messages by proposed scheme. In some cases RS estimation was greater than zero, but the value was very small and is in the range of expected deviation which even a non-stego image can produce. These results prove that dual statistic steganalysis cannot detect stego images created by the proposed steganalysis scheme.

Furthermore, our results have been endorsed by the studies of Shen *et al*. (2015) and Lu *et al.* (2017) who proposed that pixel value differencing and LSB substitution can produce superior results in terms of high payload and imperceptibility.

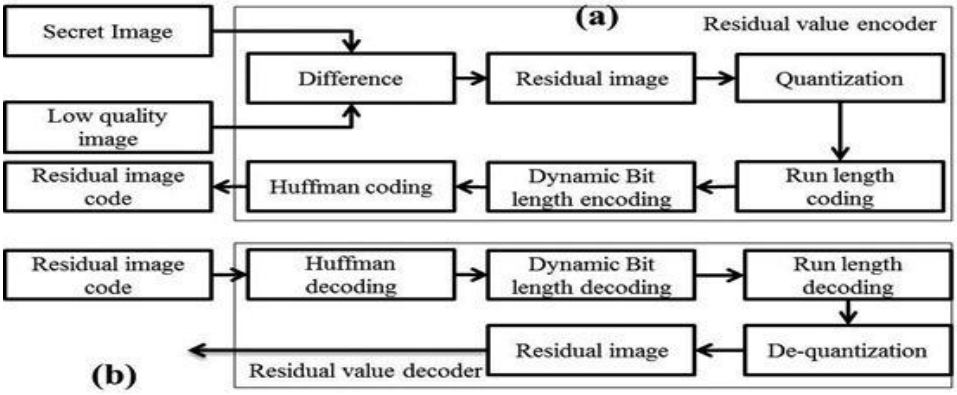


Figure 1: Block diagram of JPEG2000

a) Compression process b) De-compression process

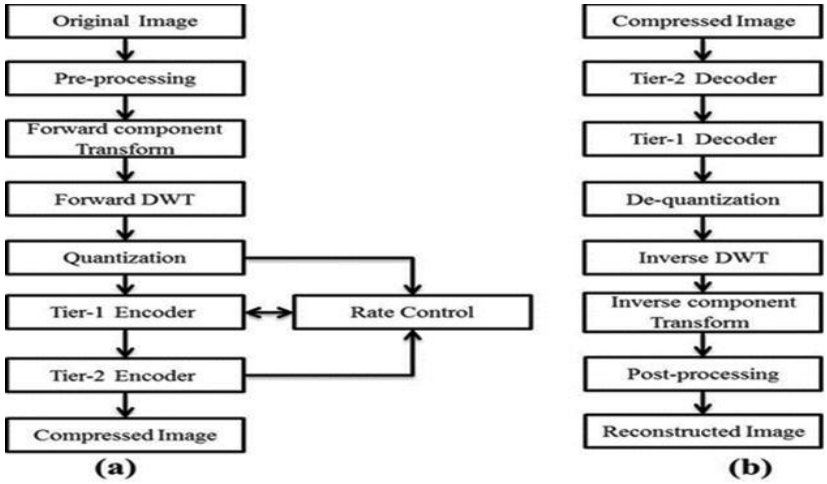


Figure 2: Block diagram of residual value coder and decoder

a) Coder b) Decoder

Figure 3: Partition of cover image

a) Cover image lena b) Partition of cover image into four sub-images

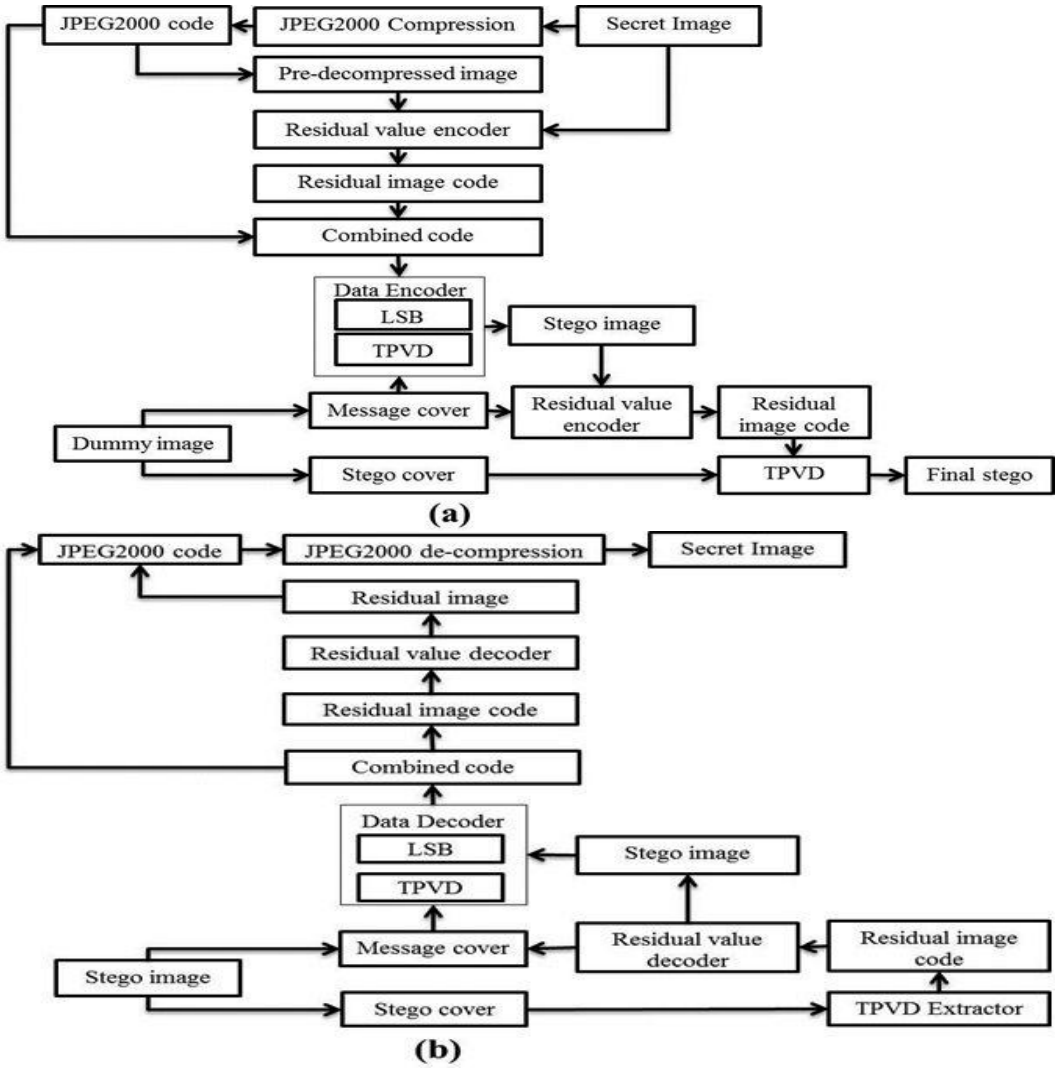
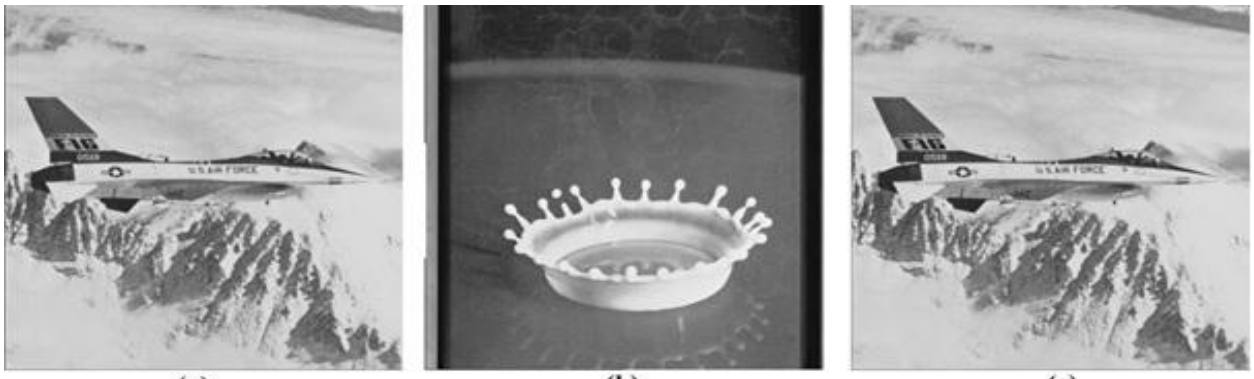


Figure 4: Block diagram of proposed scheme

a) Data embedding process b) Data extraction process

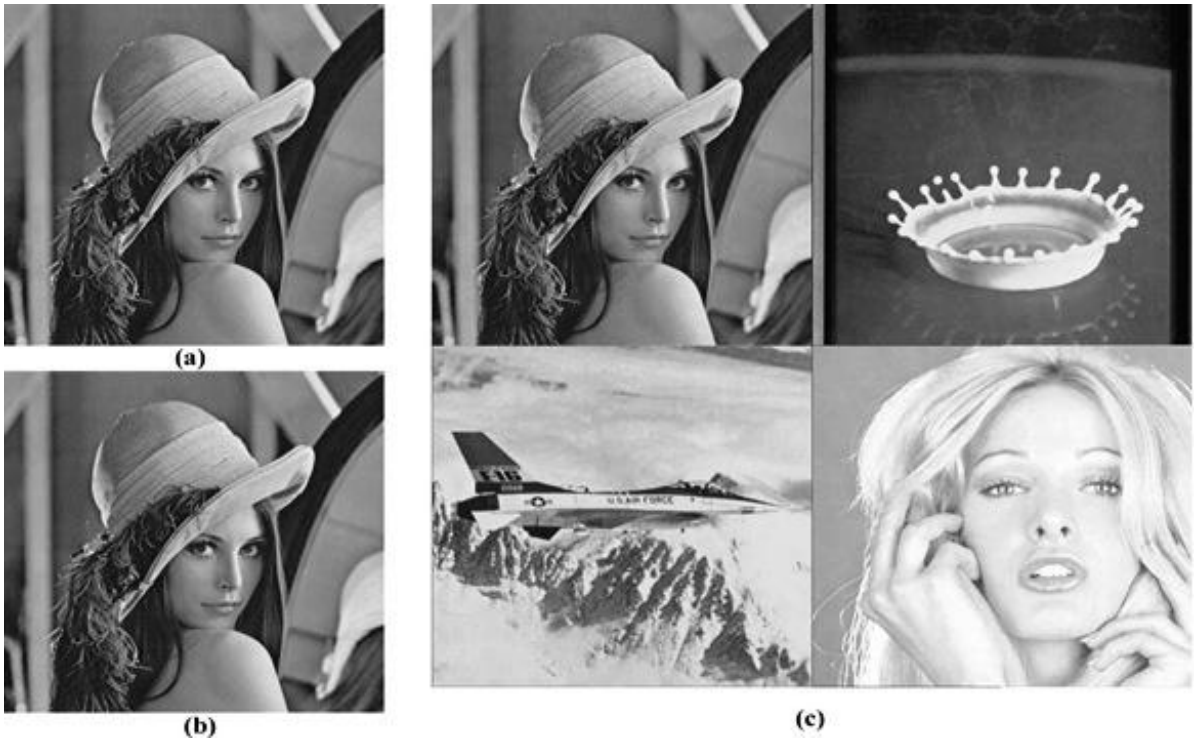


(a) (b) (c)

Figure 5: a) Jet image (cover) b) Milk image (secret message) c) jet image (stego) with PSNR 42.55 dB

(a) (b) (c)

Figure 6: a) Tiffany image (cover) b) Jet image (secret message) c) Tiffany image (stego) with PSNR 44.02 dB



(a) (b) (c)

Figure 7: a) Lena image (cover) b) 1024x1024 image (secret message) c) Lena image (stego) with PSNR 41.90 dB

Table 1. Quality of the stego-images in terms of PSNR for suggested scheme and Lee's scheme.

Secreaawt images	Size in Bytes (JPEG2000 compressed code + RIC)	Cover Images (Proposed Scheme/Lee's Scheme)			
		Lena	Jet	Milk	Tiffany
Lena	47165	_	44.26/40.04	45.01/41.49	42.74/40.59
Jet	53701	44.94 /39.97	_	45.66/40.85	44.02/40.03
Milk	25438	43.03/43.92	42.55/44.66	_	42.45/43.50
Tiffany	56242	44.45/39.78	43.32/38.93	46.9/40.52	_
Big Image1024x1024	72065	41.90/38.37	41.08/38.76	41.67/39.01	41.45/38.44

Table 2. Maximum Payload capacity of the stego-images and their quality for the proposed scheme and TPVD scheme.

Cover images 512x512 Gray-scale	TPVD		Proposed scheme	
	Capacity in bytes	PSNR in dB	Capacity in bytes	PSNR in dB
Lena	75836	38.89	80507	41.73
Baboon	82407	33.93	84351	39.96
Jet	76352	38.70	80730	41.99
Pepper	75579	38.50	78897	41.10

Table 3: Real length of embedded secret message by proposed scheme and estimated length by RS steganalysis.

Cover images	Lena	Jet	Baboon
Secret images	Big image and its RIC	Big image and its RIC	Big image and its RIC
Real length	94%	93.7%	90%
RS estimation	2.5%	0.3%	-0.013%
Cover images	Milk	Tiffany	Pepper
Secret images	Big image and its RIC	Big image and its RIC	Big image and its RIC
Real length	98.2%	95.4%	94%
RS estimation	4.2%	-0.06%	3.7%

Conclusion: A hybrid steganography scheme with high payload can be used to hide larger secret images than the cover image itself. The experimental results verify that proposed scheme provides higher payload with better PSNR than TPVD scheme.

REFERENCES

Adams, M.D., H. Man, F. Kossentini and T. Ebrahimi (2013). JPEG 2000: The next generation still image compression standard. ISO/IEC JTC, 1.

Chang, C.C., W.C. Wu and Y.H. Chen (2008). Joint coding and embedding techniques for multimedia images. Info. Sci. 178(18): 3543–3556.

Chang, K.C., C.P. Chang, P.S. Huang and T.M. Tu (2008). A Novel Image Steganographic Method Using Tri-way Pixel-Value Differencing. J. Multi. 3(2): 37–44.

Das, P., S.C. Kushwaha and M. Chakraborty (2015). Multiple embedding secret key image steganography using LSB substitution and Arnold Transform. In *2nd ICECS*, IEEE pp. 845–849.

Fridrich, J., M. Goljan and R. Du (2001). Reliable Detection of LSB Steganography in Grayscale and Color Images. Proc. of the ACM Workshop on MMSec pp. 27–30.

Gulve, A.K. and M.S. Joshi (2015). An image steganography method hiding secret data into coefficients of integer wavelet transform using pixel value differencing approach. Math. Prob. in Engg. pp. 1–11.

Haiying, G., X. Yin and L. Xu (2008). A Steganographic Algorithm for JPEG2000 Image. In Computer Science and Software Engineering, Intl. Conf. IEEE, pp. 1263-1266.

Hsieh, Y.P., C.C. Chang and L.J. Liu (2008). A two-codebook combination and three-phase block matching based image-hiding scheme with high embedding capacity. Patt. Recog. 41(10): 3104–3113.

Lee, Y.P., J.C. Lee, W.K. Chen, K.C. Chang, J. Su and C.P. Chang (2012) High-payload image hiding with quality recovery using tri-way pixel-value differencing. Info. Sci. 191: 214–225.

Lu, T.C. and Y.C. Lu (2017). An Improved Data Hiding Method of Five Pixel Pair Differencing and LSB

Substitution Hiding Scheme. Proceeding of the Twelfth Intl. Conf. on IIH and MSP 1:67-74.

Sadek, M.M., A.S. Khalifa and M.G.M. Mostafa (2015). Video steganography: a comprehensive review. Mult. T. App. 74(17): 7063–7094.

Sanjith, S., R. Ganesan and R.S.R. Isaac (2015). Experimental Analysis of Compacted Satellite Image Quality Using Different Compression Methods. Adv. Sci. Engg. Med. 7(3): 227–233.

Shen, S.Y. and L.H. Huang (2015). A data hiding scheme using pixel value differencing and improving exploiting modification directions. Comp. & Sec. 48:131-141.

Voloshynovskiy, S., S. Pereira, T. Pun, J.J. Eggers and J.K. Su (2001). Attacks on Digital Watermarks : Classification , Estimation-based Attacks and Benchmarks. IEEE Comm.Mag. 39(8): 118–127.

Wu, H.C., N.I. Wu, C.S. Tsai and M.S. Hwang (2005). Image steganographic scheme based on pixel-value differencing and LSB replacement methods. IEE Proc. Vis. Img. Sig. Process. 152(5): 611–615.