International Journal of Latest Trends in Engineering and Technology
Vol.(8)Issue(1), pp.486-493
DOI: http://dx.doi.org/10.21172/1.81.062
e-ISSN:2278-621X

SECURED STEGANOGRAPHY METHODOLOGY USING COMBINED ENCRYPTION AND QUICK RESPONSE CODES

`Dr. V. R. Sasikumar[1] and Dr. R. Vijayanandh[2]

Abstract*:* Transferring secret message is a real issue and is the need of the time. Steganography deals with concealing secret message in the image whereas cryptography is about changing the message into a distorted form, so that it is prevalent from hacker entry. Combining both the steganographic and cryptographic methodologies will yield a secure and sophisticated method for interchanging the secret messages within the transmitter and receiver. An original Discrete Wavelet Transform – Singular Value Decomposition (DWT-SVD) based stenographic methodology is accordance. Quick Response (QR) secret message payload prototypes the interchange of the singular-quantity of DWT blocks. In this document, a secure materials model is accordance by combining cryptography and steganography. QR secret messages are engagement for encoding the encrypted message. A nested image steganography is performed with QR secret messages on a suitable cover image. The suggested process has a potential to be engagement in communicating secret materials. This method has high Peak Signal to Noise Ratio (PSNR), Mean Square Error (MSE) and Root Mean Square Error (RMSE) survived chi-square quantity with 100% message recovery.

I. INTRODUCTION

Due to advancements in communicating methods and proliferation of internet facilities, it is a necessity to raise a method for transferring secret message securely over a connecting. Steganography involves concealing messages in images which are referred as cover images. These cover images are then transferred across the connecting securely. The embedded messages are overlooked and cannot be recovering without knowing the exact steganographic cover methodology. Cryptography functions modifying the message arrangement by dispense different methodologies and finally rendering a deformed message which is not intelligible. Both the methodologies have their own pros and cons. By combining both the methodologies, a secure and more sophisticated method can be built. Multimedia content and methods are rapidly increasing in the industrial integrated area. Materials secrecy of such content is of a high significance.

Cryptography comes with different solutions; however, it has been proven that it can be broken by the steady progress of the art [1][20]. Therefore, considering robust and branch choices are unavoidable. One possible feasible choice is digital steganography. Steganography is an art of embedding secret message in an innocent looking container called cover message. This cover message may be any digital media such as digital image, audio, movie folder etc. Usually the embedded secret message is called payload.

Once the payload has been embedded into a cover media it may be transmitted to the receiver or posted in public place from where intended receiver can download it. Multimedia message passing in cell and iPhone are getting more popular day by day and transmitting secret message with stego-image would be an interesting addition.

Steganography methodologies have been elaborated using the different digital image folder arrangement. In the special activity, the most popular process is the Least Significant Bit (LSB). There exist several variations of this

[1] *School of Information Technology Institute of Business Studies, Enga, Papua New Guinea*
[2] *School of Information Technology Institute of Business Studies, Port Moresby, Papua New Guinea*

process [2], [22]. Chung et al. [3], [23] for instance, suggested a singular quantity disintegration and vector quantization based image steganography with 37.002 dB PSNR. However, spatial activity steganography is venerable to blind steganalysis, explanation easily detected by statistical analysis such as chi-square quantity.

On the other hand, DWT based methods are still in its infancy for steganography. Chen et al. [4][15] suggested a DWT based image steganography scheme where they embed their secret message in the high frequency components of the DWT using 2 LSB substitutions with wavelet coefficients of *LH*, *HL*, and *HH* Sub divisions.
They obtained stego-image with PSNR difference in the limit 39.0033 dB to 54.94 dB; however, they did not report any steganalysis on their method. Driskell et al. [5] achieve high image fidelity using Daubechie wavelet filter by substituting wavelet coefficients that fall below a threshold with secret messaged letters. They also did not report any steganalysis on their method. The literature is scarce on methods that combine DWT-SVD on image steganography and has no QR-secret message steganographic methods.

II. LITERATURE SURVEY

The Advanced Encryption Standard (AES), also referred as Rijndael algorithm, is an effective cryptographic methodology widely engagement to protect integrated message. The design principle involved in AES is referred as substitution permutation connecting. The AES hidden is an iterative process, with varying data sizes (128, 192, and 256 bits). Padmavathi et al. [8][26] conducted a performance analysis survey on different methodologies like Data Encryption Standard (DES), AES, RSA combining with LSB substitution methodology which serves well to draw conclusions on the three hidden methodologies based on the their performances in any effort.
It has been concluded from their work that AES hidden is better than other methodologies as it accounts for less hidden, extraction times and also uses less buffer space. Salim M. Wadi et al. [9][24] accordance a rapid hidden method based on AES methodology for grey scale HD image hidden. The stages in AES, impart confusion, diffusion, non-linearity and obscurity to the given enter message. Quick Response secret messages alias QR secret messages are increasingly used now-a-days. Invented by Denso-Wave in 1994 QR secret messages are handy, portable and can be created efficiently.
The QR secret messages provide big space for encoding. Damir Omerasevic et al. [10][12] suggested an implementation of secure data exchange by using QR secret messages. They coined the term RISA which stands for Robustness, Integrity, Secretary and Authentication. Addition of robustness to the message communication, which is achieved by the utilization of QR secret messages, is the originality of their suggested work.
QRs have been widely accepted as they are being used by big number of efforts on iOS and Android mobile platforms due to the advancements in Smartphone technology. Yin-Jen Chiang et al. [11] suggested a new and efficient steganographic QR secret message methodology which maintains the robustness of QR secret messages by preserving the content readability of QR secret messages and also by holding the fault correction ability. The QR secret messages can be created easily and the decoding can be easily taken out with help of a smart phone equipped with a camera and a suitable decoding effort.
The QR secret messages come with a predefined structure, with specific allocations for materials in encoding the message. QR secret messages also provide other desirable features like small size, resistant to dirt and damages. And also it is readable from any guidance. Peter Kieseberg et al. [12][24] in their document explained the QR secret message security. Their work analyzed QR secret messages and their utilization to mislead automation methods and human senses. Image scrambling is a way which deals with securing the picture materials by scrambling the image into an ambiguous arrange mention. Image scrambling aims to mitigate security issues related to images.
In image scrambling and descrambling, it is necessary to have simple methodology to ‘shuffle’ the pixel quantity and reorder it to reveal the original. A pseudorandom sequence can be used to generate a scramble order. The amount of scrambling achieved determines the amount of distortion in the image. Uma Maheswari et al. [13][25] suggested a frequency activity image steganographic methodology, with the help of QR secret message and transform. QR secret message has been utilized effectively for encoding the secret message and also scrambling methodology has also been engagement to enhance the security.
Mostly scrambling processes are grounded on Arnold Transform or on a combination of Arnold Transform and other methodologies. The data based scrambling methodologies are also reliable, where a data is created which is

shared by both parties to communicate. Somdip Dey et al. [14][30] suggested an advanced steganography methodology for embedding the message which involves message to undergo hidden, encoding into QR secret messages, scrambling and then embedding into cover image.

The Least Significant Bit methodology is applied to imbed the bits of the secret message in a deterministic sequence, straight into the LSB (Least Significant Bit) plane of an image, referred as cover image. As the measure of the change is not much, varying the least significant bits does not lead to a human perceptible difference. LSB method comes with easy implementation and acceptable outputs. Wai Wai Zin [15][22] suggested in his work, and embedding scheme for messages using LSB steganographic methodology. Kaustubh choudhary et al. [16][17] accordance a detailed report on image properties in LSB plane.

His work describes the bit plane slicing methodology in detail, which summarizes the significances of MSB and LSB planes of an image. In this section, Hu and Jeon first suggested a reversible visible watermarking scheme by modifying one significant bit plane of the pixels of the host image. They achieved reversibility via embedding the compressed version of the altered bit plane without loss into the non-watermarked image region. However, the embedded visible watermark with this method appears to be somewhat blurred, and the visual quality of the original image is significantly deformed.

There are two procedures in this methatology: message embedding and visible watermark embedding. the framework of the suggested methatology. *W* and *R* denote the visible watermark and the image region to be protected, respectively. *W* has the same size as *R*. To achieve lossless recovery of the image *I*, the bit plane of *R* must be preserved in the non-watermarked image area *I-R* before *W* is embedded into a bit plane of *R*. In Stage 1, the bit plane of *R* constitutes the pixel set *D*. A bit-plane message usually has a statistical structure, so D is further compressed into *Dc* in Stage 2 using the open C secret message of JBIG-KIT.

III. PROPOSED METHOD

The use of QR secret messages in steganography [10-14] is not original but the originality of the suggested methodology lies in the utilization of QR secret messages for achieving security levels in transmitting the secret message. This methodology imparts security levels on the secret message to be transferred securing it efficiently. Fig. 1 shows the framework for the proposed methodology.

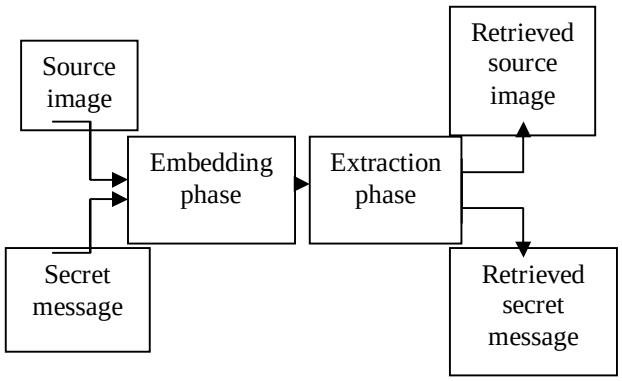

Figure 1. Framework for the proposed methodology

The devised method is categorized into four segments at both transmitter's side as well as receiver's side.

3.1 Quick Response (QR) Code

QR secret message was introduced by Denso Wave in 1994. It is a 2-D secret message with control points that makes it easier to be interpreted by scanning equipment such as smart phones, digital camera and hand held scanner. Moreover, QR secret message fault correction ability makes it ideal for steganography. For different version of QR secret message, there are different segment configurations where segments refer to the black and white dots which construct the QR Secret message. The biggest standard QR Secret message is V-40 symbol, which is 177x177 segments in size and can hold up to 4296 characters of alphanumeric message. The structure of the QR secret message is shown in Fig. 2.

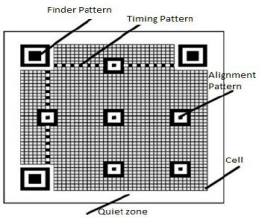

Figure 2. Structure of the Quick Response Secret message

3.2 Transmitter's Side

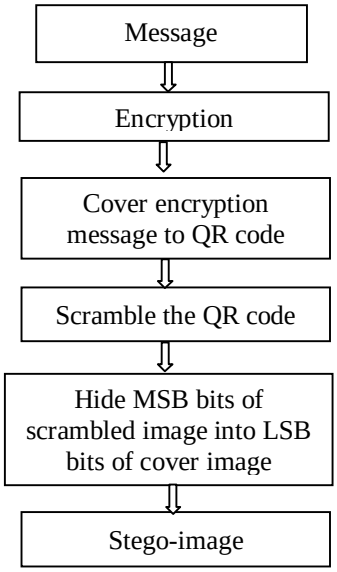

Figure 3. Block diagram for transmitter's side procedure

The four segments at the transmitter's side are,

3.2.1 Encryption:

The first segment at the transmitter's side encrypts the secret message using data hidden methodology [9]. The encrypted message, in USV arrangement is converted in to arrangement to make it compatible for further processing, which is then written in to the folder and stored for further processing.

3.2.2 Encoding:

The second segment ensured messages the encrypted text (base64 arrangement) in to QR secret message [14]. For the encrypted text written in to the folder, a unique QR secret message is created. The QR encoding is unique and serves well for embedding the message.

3.2.3 Scrambling:

The third segment generates a scramble order at random which along with the extracted RGB quantity is stored [16]. The random scramble order is applied on the RGB quantity extracted from the image and the same is communicated to the receiver's side. The resulting quantity of the scramble function are reshaped according to the image size (Rows *Columns). Finally a scrambled image is created concatenating the three RGB quantities and then generating an image from it.

3.2.3 Embedding

A steganographic methodology using DWT and SVD transform is suggested. We use a QR secret message generator to produce a payload (secret message) which is converted to one dimensional vector with a sequence of 1's and 0's. To embed the payload in DWT sub divisions (especially the LL sub division), a degradation of the quality of the image is imminent. Hence, we chose to decompose the LL sub-division up to three levels to capture the mid-limit frequency elements in those sub-divisions (i.e., HL and LH).

HH typically contains more outside limit related materials of the image, then, the HL and LH pair is a better sub division selection. Each sub division LH and HL are divided into a numbers of non-overlapping 16x16 blocks. There is evidence that any modification on image has less effect on 1st few SVs of the SVD decomposed image [6]. In this research we used the 1-D sequence of the QR secret message to alter the quantity of σ2 with either σ1 or σ3 according to the polarity (1 or 0) of the QR secret message sequence. Fig 3 is the flow chart of the suggested methodology. The SVD of a matrix A mxn is given in equation 1 below.

$A=USV^{T}$ (1)

Where U and V are the left and right singular vectors of size m×m and n×n respectively and S = diag (σ1, σ2, .., σr) with size m×n. The diagonal matrix S, has rank r equal to the rank of A. The nonzero elements are called singular quantity of *A* and are in descending order. The singular quantity (SVs) is the square roots of the Eigen quantity of *AT.A* or *A.AT*. The suggested method can be used in iterative manner, explanation, if we cannot recover the exact payload in the first time, we re-implement the process on stego-image until we obtain the payload. We take the stego-image and substitute the following process again to ensure 100% extraction of the payload.

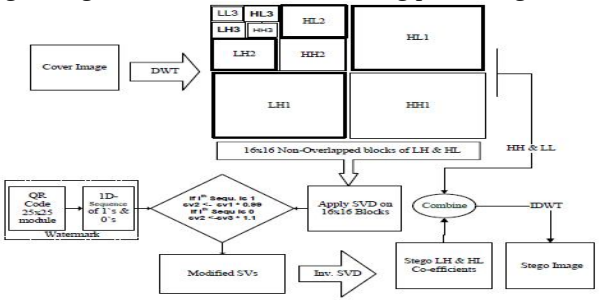

Figure 4. Block Diagram of Payload embedding

3.3 Receiver's Side

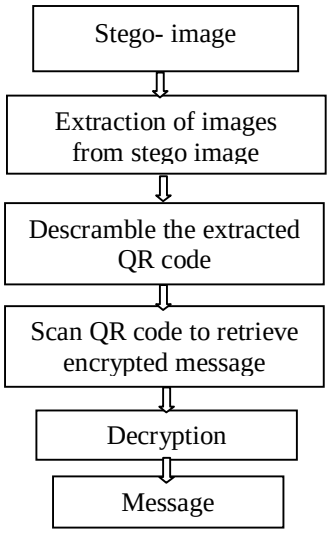

Figure 5. Block diagram of receiver's side procedure

The four segments at the receiver's side which reverse the effects imparted at the transmitter's side

3.3.1 Retrieval

The extraction process can be formulated as follows:

1. Substitute up to 3rd level DWT to the stego image *Ig.*
2. Substitute SVD on each 16x16 block of *LH1-to-3* and *HL1-to-3* sub division of image *Ig*.
3. Find the ratio within the 1st and 2nd singular quantity of each block of *Ig*. Extracted quantity is then map into extracted one dimensional payload using the following equation:

$$EP_i = \begin{cases} 1 & if \frac{\sigma 1}{\sigma 2} > T \\ 0 & if \frac{\sigma 1}{\sigma 2} < T \end{cases} \quad (2)$$

Where the quantity of *T* (threshold) in the limit. Finally one-dimensional EPi is converted into 25x25 matrixes to construct the version-2 QR secret message.

3.3.2 Descrambling

The recover image, which is scrambled, is then descrambled using the descrambling methodology and the received random created sequence. First the scrambled image is loaded and a reverse order is created from the folder containing the scrambling order materials. The RGB matrix quantity is then arranged according to the newly created reverse order. The required QR secret message image can be created by concatenating this quantity to form an image. The coding specifications for descrambling are the same as scrambling. All the functions are inverted in the process.

3.3.3 Scanning

The descrambled QR secret message is then scanned to get the ensured messaged materials, which is here, the secret message in encrypted form. The scanning can be easily taken out, with the help of mobile apps. They are handy and can be easily downloaded and installed. They use the mobiles built in camera and a decoding program to scan and display the content of the ensured messaged QR secret message.

3.3.4 Decryption

The final phase, Extraction involves decrypting the encrypted message, to retrieve the original materials. It takes the same 16 character data, which is used to encrypt the message at the transmitter's side. The recover message is then delivered to the person concerned.

IV. RESULTS AND DISCUSSION

The security is enhanced by employing hidden methodology and utilizing the QR secret message. The encrypted message is hard to break and the QR secret message is secured by dispense scrambling methodology to it. The stego image created and the cover image are similar with no human perceptible faults.

The different images quantities with suggested methodology and show the stages in the hidden process. It is evident from the results that the stego image created is similar to the cover image and cannot be identified by a human eye. Also it can be proved from the tabulated MSE (Mean Square Fault) and RMSE (Root Mean Square Fault) quantity of the selected images in Table 1 that the stego images do not deviate much from the cover image after dispense the suggested methodology and are reliable for transferring the materials across a connecting.

Table.1. Mean square error and root mean square error values of the selected images.

IMG NO	MSE	RMSE	PSNR in dB
1	0.928	0.9621	40.31
2	0.9338	0.9663	35.84
3	0.8821	0.9122	40.52
4	0.8660	0.9306	33.56
5	0.6420	0.8012	36.24

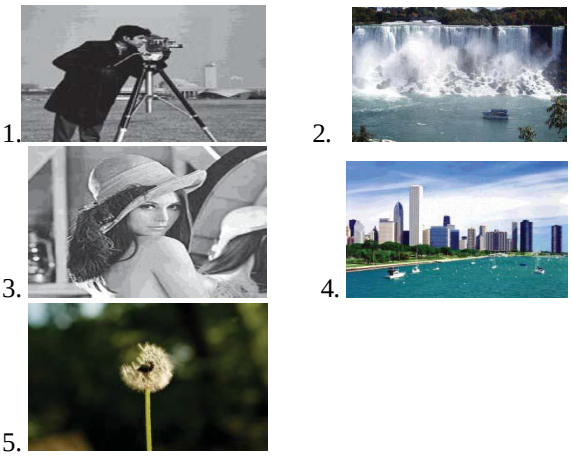

Figure 6. Selected Images

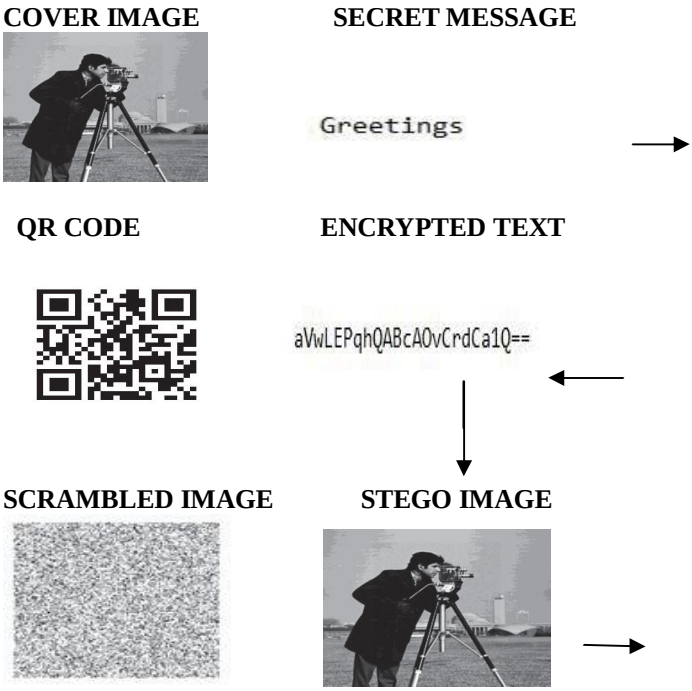

Figure 7. Stages involving in encryption

V. CONCLUSION

The suggested method suggests a combination of strong encrypting methodology and steganographic methodology to make the communication of secret materials safe, secure and extremely hard to desecrate message. A hidden methodology is engagement to encrypt a secret message before encoding it in to a QR secret message. An original QR secret message guided DWT-SVD steganographic methodology for consumer and business efforts is accordance. We altered the 2nd SV of DWT blocks' quantity in such a way that it does not change the stego-image quality and it does not violate the SVs ($\sigma 1, \sigma 2, \ldots, \sigma r$) order. Also, we have introduced QR-secret message as payload to guide the alteration of 2nd SV. We exploited the QR secret message self-correcting ability of up to 7% to reach 100% message recovery.

The ensured messaged image is scrambled to achieve another security level. The scrambled QR secret message is finally embedded in a suitable cover image, which is then transferred securely to deliver the secret materials. At the receiver's side the secret materials is recover through the decoding process. Thus, a four level security has been rendered for the secret message to be transferred. This methodology is applicable to security mechanisms which serve to communicate secret materials in banking, defence, educational, e-Business sectors. The suggested methodology can be further improved to enhance the security by adopting different modifications to the segments, as required.

REFERENCES

[1] B. Li, J. He, J. Huang, Y. Q. Shi, 'A Survey on Image Steganography and Steganalysis', Journal of Information Hiding and Multimedia Signal Processing, vol. 2, no. 2, 2011, pp 142-172.

[2] A. Cheddad, J. Condell, K. Curran, P. M. Kevitt, 'Digital Image Steganography: Survey and Analysis of current methods', Signal Processing, Elsevier, 90(2010), pp 727-752

[3] K. L. Chung, C H Shen, L. C. Chang, "A novel SVD and VQ-based image hiding scheme", Pattern Recognition Letters, vol. 22, 2001, pp 1051-1058.

[4] P. Y. Chen, and H. J. Lin, "A DWT based approach for image steganography", International Journal of Applied Science and Engineering, vol. 4, no. 3, 2006, pp. 275-290.

[5] L. Driskell , "Wavelet based steganography", Cryptologia, Taylor & Francis, 28:2, 2010, pp. 157-174.

[6] M. W. Islam, S. alZahir, "A robust color image watermarking scheme", in IASTED Intl. Conf. on Visualization, Imaging, and Image processing, VIIP 2012, Banff, Canada, July 3-5, 2012.

[7] A. Noore, N. Tungala, and M. M. Houck, " Embedding biometric identifiers in 2D barcodes for improved security," Computers & Security, 23 (8) 679-686 (2004).

[8] B. Padmavathi, S. Ranjitha Kumari " A Survey on Performance Analysis of DES, AES and RSA Algorithm along with LSB Substitution", International Journal of Science and Research (IJSR), India Online ISSN: 2319-7064
[9] Salim M. Wadi, Nasharuddin Zainal " Rapid Encryption Method based on AES Algorithm for Grey Scale HD Image Encryption", 4th International Conference on Electrical Engineering and Informatics, ICEEI 2013.
[10] Damir Omerasevic, Narcis Behlilovic, Sasa Mrdovic, "An Implementation of Secure Key Exchange by Using QR Codes", 56th International Symposium ELMAR-2014, 10-12 September 2014, Zadar, Croatia.
[11] Yin-Jen Chiang, Pei-Yu Lin, Ran-Zan Wang, Yi-Hui Chen," Blind QR Code Steganographic Approach Based upon Error Correction Capability", KSII Transactions on Internet and Information Systems vol. 7, no. 10, Oct. 2013
[12] Peter Kieseberg, Manuel Leithner, Martin Mulazzani, Lindsay Munroe, Sebastian Schrittwieser, Mayank Sinha, Edgar Weippl "QR Code Security",2014.
[13] S. Uma Maheswari, D. Jude Hemanth "Frequency domain QR code based image steganography using Fresnelet transform", Int. J. Electron. Commun. (AEÜ) 69 (2015) 539–544.
[14] Somdip Dey, Kalyan Mandal, Joyshree Nath, Asoke Nath "Advanced Steganography Algorithm Using Randomized Intermediate QR Host Embedded With Any Encrypted Secret Message: ASA_QR Algorithm", I.J.Modern Education and Computer Science, 2012, 6, 59-67 .
[15] Wai Wai Zin," Message Embedding In PNG File Using LSB Steganographic Technique", International Journal of Science and Research (IJSR), India Online ISSN: 2319-7064.
[16] Kaustubh Choudhary," Properties of Images in LSB Plane", IOSR Journal of Computer Engineering (IOSRJCE), 2278-0661 Volume 3, Issue 5 (July-Aug. 2012), PP 08-16.
[17] M. Y. Cheng and J. C. Chen, "Integrating barcode and GIS for monitoring construction progress," Automation in Construction, 11 (1) 23-33 (2002).
[18] J. A. Stewart and F. A. Short, " Time accuracy of a barcode system for recording resuscitation events: laboratory trials," Resuscitation , 42 (3) 235–240 (1999).
[19] A. Collins, A. Zomorodian, G. Carlsson and L. J. Guibas, "A barcode shape descriptor for curve point cloud data," Computers and Graphics, 28 (6) 881-894 (2004).
[20] D. E. Gilsinn, G. S. Cheok, and D. P. O'Leary, "Reconstructing images of barcodes for construction site object recognition," Automation in Construction, 13 (1) 21-35 (2004).
[21] S.D. Lin and S.C. Shie. "Improving robustness of visible watermarking schemes for images," *the 2004 IEEE International Symposium on Consumer Electronics*, 2004, pp.011 -014.
[22] H.M. Tsai and L.W. Chang, "A high secure reversible visible watermarking scheme," IEEE International Conference on Multimedia and Expo, 2007, pp. 2106-2109.
[23] Y. Hu and S. Kwong, "Wavelet domain adaptive visible watermarking," Electron. Lett. , Vol. 37, no. 20, Sep. 2001, pp. 1219– 1220.
[24] T.Y. Liu and W.H. Tsai, "Generic Lossless Visible Watermarking—A New Approach," IEEE Transactions on Image Processing, vol. 19, May 2010, no. 5.
[25] M.J. Tsai, "A visible watermarking algorithm based on the content and contrast aware (COCOA) technique", JVCIR(20), no. 5, July 2009, pp. 323-338.
[26] H.C. Huang, F. C. Chang, and W. C. Fang, "Reversible Data Hiding with Histogram-Based Difference Expansion for QR Code Applications," IEEE Trans. Consumer Electronics, Vol. 57, no. 2, May 2011, pp. 779-787.
[27] Z. M. Lu, J. X. Wang, and B. B. Liu, "An improved lossless data hiding scheme based on image VQ-index residual value coding," The Journal of Systems and Software, Vol. 82, pp. 1016-1024, 2009.
[28] C.C. Chang, T.D. Kieu, and W.C. Wu, "A lossless data embedding technique by joint neighboring coding," Pattern Recognition, Vol. 42, no. 7, July 2009, pp. 1597-1603.
[29] Z. M. Lu, J. X. Wang, and B. B. Liu, "An improved lossless data hiding scheme based on image VQ-index residual value coding," The Journal of Systems and Software, Vol. 82, pp. 1016-1024, 2009.
[30] Y.J. Hu, S. Kwong, and J. Huang, "An algorithm for removable visible watermarking," IEEE Trans. Circuits Syst. Video Tech, Vol. 16, no. 1, Jan. 2006, pp.129–133.