ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 12, December 2014

A Contemporary Secure Data Scheme Based on Image in painting and Side Match Vector Quantization (SMVQ)

K.Sridevi[1], V.R.Anitha[2]

M.Tech Student, Dept of Electronics & Communication Engineering, Sri Vidyanikethan Engineering College, Tirupati, India

Professor, Dept of Electronics & Communication Engineering, Sri Vidyanikethan Engineering College, Tirupati, India

ABSTRACT: Data hiding and image compression techniques can be integrated into one single module seamlessly to transfer the image information securely. Data Hiding involves embedding significant data into various forms of digital media such as text audio image and video, this data is encrypted and then transferred. Image in painting technique is used to fill the missing areas or modifying the damaged regions of the received image. The project explains novel joint data-hiding and compression scheme for digital images using side match vector quantization (SMVQ) and image edge based Harmonic in painting. Before transmitting, the image is divided into many blocks. At the sender side, except for the blocks in the leftmost and topmost of the image, each of the other residual blocks in raster-scanning order can be embedded with secret data and compressed simultaneously by SMVQ or image in painting adaptively according to the current embedding bit. Vector Quantization (VQ) is also utilized for some complex blocks to control the visual distortion and error diffusion caused by the progressive compression. After segmenting the image compressed codes into a series of sections by the indicator bits, the receiver can achieve the extraction of secret bits and image decompression successfully according to the index values in the segmented sections.

I.INTRODUCTION

The rapid expansion of Internet technology, people can transmit and share digital content with each other conveniently. In order to guarantee communication competence and save system bandwidth, compression techniques can be implemented on digital content to decrease redundancy, and the excellence of the decompressed versions should also be conserved. Nowadays, most digital content, especially digital images and videos are rehabilitated into the compressed forms for transmission. Another imperative issue in an open network environment is how to send out secret or personal data steadily. Even though traditional cryptographic methods can encrypt the plaintext into the cipher text, the meaningless accidental data of the cipher text may also arouse the misgiving from the attacker. To solve this problem, in sequence hiding technique have been broadly urbanized in both academic world and industry, which can embed secret data into the cover data unnoticeably. Due to the prevalence of digital images on the Internet, how to compress images and hide secret data into the dense images efficiently deserve in-depth study. Recently, many data-hiding scheme for the compressed codes have been reported, which can be applied to various density techniques of digital images, such as JPEG, JPEG2000, and vector quantization (VQ). As one of the most accepted lossy data compression algorithms, VQ is widely used for digital image compression due to its simplicity and cost efficiency in implementation. During the VQ compression process, the Euclidean distance is utilized to evaluate the similarity between each image block and the codeword in the codebook. The index of the codeword with the negligible distance is recorded to symbolize the chunk. Thus, an index table consisting of the index values for all the blocks is generate as the VQ firmness codes. Instead of pixel principles, only the index values are stored,

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 12, December 2014

consequently, the density is achieved effectively. The VQ decompression process can be implement easily and efficiently because only a simple table lookup operation is required for each received
index. The proposed scheme in this paper is based on SMVQ. On the sender side, except for the blocks in the leftmost and secret images, in which different combinations of shares reconstruct different secrets, becomes a significant research topic. The related studies in the literature can be classified into two categories in terms of the decoding processes: (1) direct superimposition only, where the shares are stacked directly onto each other; and (2) allowing additional operation(s) before superimposition, where at least one of the shares is allowed to take one or more operations (such as flipping or rotation) before stacking onto others. Currently, the research on the first category is relatively less than the second one. Particularly, the latter has achieved the sharing of any general secrets, while the former has only involved the sharing of two secrets.

II.EXISTING METHOD

In the proposed method, a PNG image is created from a binary-type grayscale document image *I* with an alpha channel plane. The original image *I* may be thought as a *grayscale channel plane* of the PNG image. An illustration of this process of PNG image creation. Next, *I* is binarized by moment-preserving thresholding, yielding a binary version of *I*, which we denote as *Ib*. Data for authentication and repairing then are computed from *Ib* and taken as input to Shamir's secret sharing scheme to generate *n* secret shares.The share values are mapped subsequently into a small range of alpha channel values near the maximum transparency value to
create an imperceptibility effect. Finally, the mapped secret shares are randomly embedded into the alpha channel for the purpose of promoting the security protection and data repair
capabilities. Two block diagrams describing the proposed method. Since the alpha channel plane is used for carrying data for authentication and repairing, no destruction will occur to the input image in the process of authentication. In contrast, conventional image authentication methods often sacrifice part of image contents, such as LSBs or flippable pixels, to accommodate data used for authentication. In addition, once a stego-image generated from a conventional method like an LSB-based one is unintentionally compressed by a lossy compression method, the stego-image might cause false positive alarms in the authentication system. In contrast, the proposed method yields a stego-image in the PNG format which in normal cases will not be compressed further, reducing the possibility of erroneous authentication caused by imposing undesired compression operations on the stego-image.

III.PROPOSED METHOD

In the proposed scheme, rather than two separate modules, only a single module is used to realize the two functions, i.e., image compression and secret data embedding, simultaneously. The image compression in mainly on the SMVQ
mechanism. According to the secret bits for embedding, the image compression based on SMVQ. After receiving the secret embedded and compressed codes of the image, one can extract the embedded secret bits successfully during the image decompression..

A. Image enhancement

Image compression may be lossy or lossless. Lossless compression is preferred for archival purposes and often for medical imaging, technical drawings, clip art, or comics. Lossy compression methods, especially when used at low bit rates, introduce compression artifacts. Lossy methods are especially suitable for natural images such as photographs in applications where minor (sometimes imperceptible) loss of fidelity is acceptable to achieve a substantial reduction in bit rate. The lossy compression that produces imperceptible differences may be called visually lossless.

B. Data Embedding

Data hiding was introduced as part of the OOP methodology, in which a program is segregated into objects with specific data and functions. This technique enhances a programmer's ability to create classes with unique data sets and functions, avoiding unnecessary penetration from other program classes. Because software architecture techniques rarely differ, there

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 12, December 2014

are few data hiding contradictions. Data hiding only hides class data components, whereas data encapsulation hides class data parts and private methods. Information hiding for programmers is executed to prevent system design change. If design decisions are hidden, certain program code cannot be modified or changed. Information hiding is usually done for internally changeable code, which is sometimes especially designed not to be exposed. Such stored and derived data is not expounded upon, most generally. Change resilience of classes and ease of use by client objects are two byproducts of hidden data. To behavior the decompression and secret bit extraction of each remaining block, the compressed codes are segmented into a series of section adaptively according to the indicator bits. Explicitly, if the current indicator bit in the packed in codes is 0, this indicator bit and the following log2 W bits are segmented as a piece, which means this section corresponds to a VQ compressed block with no embedded secret bit. The decimal value of the last log2 W bits in this section is exactly the VQ index that can be used directly to recover the block. Otherwise, if the current indicator bit is 1, this indicator bit and the subsequent log2 $(R + 1)$ bits are then segmented as a section, which means this section corresponds to an SMVQ or inpainting compressed block. Denote the decimal value of the last log2 $(R + 1)$ bits in this section as λ'. Under this condition, if λ' is equal to R, it implies that the residual block parallel to this section was compressed by inpainting and that the embedded secret bit in this block is 1. Otherwise, if $\lambda' \in [0, R-1]$, it imply that the block matching to this section was compressed by SMVQ and that the entrenched secret bit is 0. After all the segmented sections in the packed in codes complete the above describe procedure, the embedded secret bits can be extracted correctly, and the decompressed image $\mathbf{I}d$ can be obtain successfully. Due to the decoding of the compressed codes, the decompressed picture $\mathbf{I}d$ doesn't surround the embedded secret bits any longer. Note that the process of secret bit extraction can also be conducted separately, the data embedding technique may be used for many algorithms one of the best technique is side match vector quantization technique which means that the receiver can obtain all embedded bits by simply segmenting and analyzing the compressed codes without the decoding. the receiver can obtain the secret bits at any moment if he or she conserve the compressed codes. The proposed scheme can also be used for the integrity corroboration of the images, in which the secret bits for embedding can be regarded as the hash of the image attitude contents. The receiver can calculate the hash of the principle contents for the decompressed picture, and then compare this calculated hash with the extracted secret bits (embedded hash) to judge the integrity of the received compressed codes and the corresponding decompressed image. If the two hashes are equal, it earnings the image is genuine. Otherwise, the received compressed codes must be tampered.

IV.EXPERIMENTAL RESULTS

Fig.1 Original image

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 12, December 2014

Fig.2 Secret image

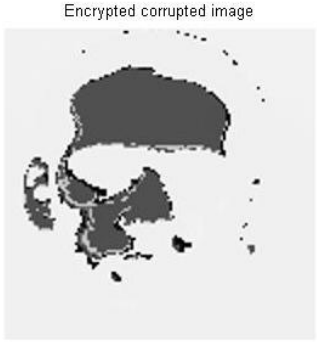

Fig.3 Encrypted corrupted image

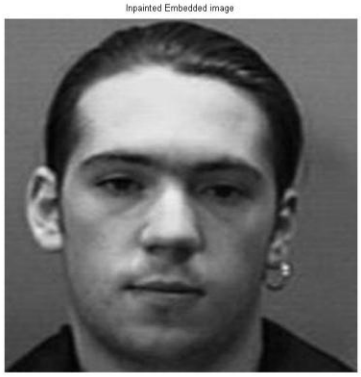

Fig.4 In painted Encrypted image

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 12, December 2014

Fig.5 Encrypted image

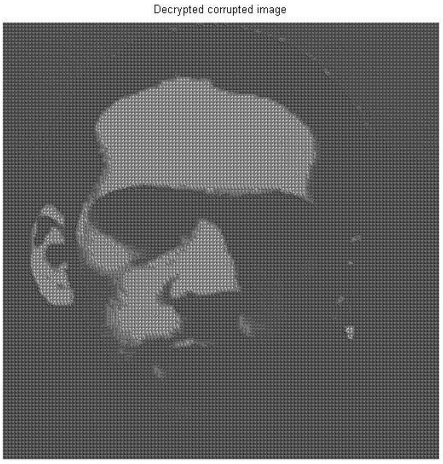

Fig.6 Decrypted corrupted image

Fig.7 Secret image

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 12, December 2014

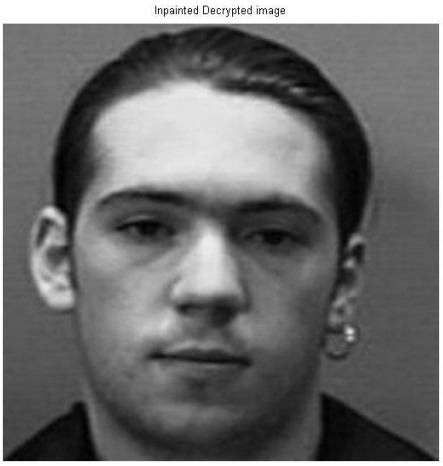

Fig.8 In painted Decrypted image

V.CONCLUSION

In this paper, we proposed a joint data-hiding and compression scheme by using SMVQ and PDE-based image Arnold decoding. The blocks, except for those in the leftmost and topmost of the image, can be embedded with covert data and packed in at the same time, and the adopted compression method switches between SMVQ and SVD adaptively according to the embed bits. SVD (singular value decomposition) is also utilized for some complex blocks to control the visual distortion and error dissemination. The SVD method may be used for better results coming to existing system. On the recipient side, after segmenting the packed in codes into a series of sections by the indicator bits, the embedded secret bits can be easily extract according to the index values in the segmented sections, and the decompression for all blocks can also be achieved productively by VQ, SMVQ, and Arnold coding. The experimental results show that our scheme has the acceptable performance for hiding capacity, compression ratio, and decompression quality. Furthermore, the proposed scheme can integrate the two functions of data hiding and image compression into a single module seamlessly. In feature work would be better results coming to receiver and transmitter part.

REFERENCES

[1] W. B. Pennebaker and J. L. Mitchell, *The JPEG Still Image Data Compression Standard*. New York: Reinhold, 1993.
[2] D. S. Taubman and M.*EG2000: Image Compression Fundamentals Standards and Practice*. Norwell, MA: Kluwer, 2002.
[3] A. Gersho and R. M. Gray, *Vector Quantization and Signal Compression*. 1992.
[4] N. M. Nasrabadi and R. King, "Image Coding Using Vector Quantization: A Review," *IEEE Transactions on Communications*, pp. 957-971, 1988.
[5] National Institute of Standards & Technology, "Announcing the Advanced Encryption Standard (AES)," *Federal*
[6] R. L. Rivest, A. Shamir and L. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems,"
[7] F. A. P. Petitcolas, R. J. Anderson and M. G. Kuhn, "Information Hiding — A Survey," 87, no. 7, pp., 1999.
[8] C. D. Vleeschouwer, J. F. Delaigle and B Macq, "Invisibility and Application Functionalities in Perceptual Watermarking:
[9] C. C. Chang, T. S. Chen and L. Z. Chung, "A Steganographic Method Based
Sciences, vol. 141, no. 1, pp. 123-138, 2002.
[10] H. W. Tseng and C. C. Chang, "High Capacity Data Hiding in JPEG-Compressed Images,"., 2004.
[11] P. C. Su and C. C. Kuo, "Steganography in JPEG2000 Compressed Images4, pp. 824-832, 2003.
[12] W. J. Wang, C. T. Huang and S. J. Wang, "VQ Applications in Steganographic Data Hiding Upon Multimedia Images," *IEEE* 5, no. 4, pp. 528-537, 2011.
[13] Y. C. Hu, "High-Capacity Image Hiding Scheme Based on Vector Quantization," *Pattern Recognition*, vol. 39, no. 9, pp., 2006.
[14] Y. P. Hsieh, C. C. Chang and L. J. Liu, "A Two-Codebook Combination
and Three-Phase Block Matching Based Image-Hiding Scheme with High Embedding Capacity," *Pattern Recognition*, vol. 41,no. 10, pp. 3104-3113,

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 12, December 2014

2008.
[15] C. H. Yang and, "Fractal Curves to Improve the Reversible Data Embedding for VQ-Indexes Based on Locally Adaptive Coding," *and Image Representation*, vol. 21, no. 4, pp-342, 2010.
[16] Y. Linde, A. Buzo and R. M. Gray, "An Algorithm for Vector Quantization Design," *IEEE Transactions on Communications*, vol., 1980.
[17] C. C. Chang and W. C. Wu, "Fast Planar-Oriented Ripple Search Algorithm for Hyperspace VQ Codebook," *IEEE* 2007.
[18] W. C. Du and W. J. Hsu, "Adaptive Data Hiding Based on VQ Compressed Images," *IEE Proceedings - Vision, Image and Signal*, no. 4, pp. 233-238, 2003.
[19] C. C. Chang, "Hiding Secret Data Adaptively in Vector Quantisation Index Tables
[20] C. C. Lin, S. C. Chen and N. L. Hsueh, "Adaptive Embedding Techniques for VQ-Compressed Images," *Information Sciences*, vol. 179, no. 3, pp. 140-149,
[21] C. H. C. Tsai, "Lossless Compression of VQ Index with Search-Order Coding," *IEEE Transactions on Image Processing*, vol. 5, no. 11, pp. 1579-1582, 1996.
[22] C. C. Lee, W. H. Ku and S. Y. Huang, "A New Steganographic Scheme Based on Vector Quantisation and Search-Order Coding," *IET Image Processing*, vol. 3, no. 4, pp, 2009.
[23] S. C. Shie and S. D. Lin, "Data Hiding Based on Compressed VQ Indices of Images," *Computer Standards Interfaces*, vol. 31, no. 6, pp. 1143-1149, 2009.