International Journal for Modern Trends in Science and Technology, 7(04): 132-136, 2021

ISSN: 2455-3778 online
DOI: https://doi.org/10.46501/IJMTST0704020
Available online at:http://www.ijmtst.com/vol7issue04.html

Information Masking using Digital Keys for Sports Auction

Nethrashruthi R[1] | Rasiga R[1] | Shalini M[1] | Sinekha S[1] | R.Ashwini[2]

[1]UG Students, Department of C.S.E, Jansons Institute of Technology, Coimbatore, India.
[2]Assistant Professor, Department of C.S.E, Jansons Institute of Technology, Coimbatore, India.

To Cite this Article
Nethrashruthi R, Rasiga R, Shalini M, Sinekha S and R.Ashwini, "Information Masking using Digital Keys for Sports Auction", *International Journal for Modern Trends in Science and Technology*, Vol. 07, Issue 04, April 2021, pp.:132-136.

Article Info
Received on 18-March-2021, Revised on 02-April-2021, Accepted on 10-April-2021, Published on 17-April-2021.

ABSTRACT

It is a novel approach for Information Masking using a reversible texture synthesis. A texture synthesis process re-samples a smaller texture image which synthesizes a new texture image with a similar local appearance and arbitrary size.The texture synthesis process into masking with image to conceal secret messages using RSA algorithm for encryption. In contrast to using an existing cover image to hide messages, our algorithm conceals the source texture image and embeds secret messages through the process of texture synthesis. This allows us to extract secret messages and the source texture from a stego synthetic texture.High volumetric data is embedded into bit-planes as low as possible to keep message integrity, but at the cost of an extra bit-plane encoding procedure and slightly changed compression ratio. The proposed method can be easily integrated into the JPEG2000 image coder, and the produced stego-bit stream can be decoded normally.

KEYWORDS: *Quantum Information Processing, Twice bit-plane encoding, Rate-distortion optimization, Scrambled synchronization, Message extraction*

I. INTRODUCTION

The protection of masking a sensitive data using digital key represents an urgent need for secure communications, especially in today's innovative and modern information and communication technology. It is a new paradigm and an incredible technology for equipping quickly deployable and scalable information technology solutions at conservative network bandwidth, reduced infrastructure costs, low latency, location awareness, and mobility support.

It is a trusted and dependable solution to bring the services and resources of the cloud closer to users and thus assists in leveraging the available services and resources in the edge networks. However, emerged internet services lead to privacy and security issues and challenges. Transmitting secret data through unsecured and open channels, as in fog IoT, is an issue that should be addressed. One of the solutions for dealing with the security concerns, especially the handling of masking data covertly in the Internet based computing paradigm, is via quantum information processing (QIP).

QIP has received considerable attention from scientists devoted to development and those interested in introducing novel quantum approaches for processing, storing, and transmitting quantum information. In recent years, some papers have focused on several key topics of QIP, such as quantum coding, quantum teleportation, quantum cryptography and quantum steganography, among many others for masking the information. The aim of quantum steganography is to transfer classical or quantum data covertly via open channels.

II. PURPOSE

The main purpose of the system is to improve the security by using RSA algorithm and for hiding and compressing the capacity in JPEG2000 wavelet transform (DSP) is used.

III. SCOPE

The system scope includes the following

- To reliably embed high-volume data into the JPEG2000 bit-stream
- To encryption data hide to image using wave let transformer. It is gives high performance
- To encryption data hide to image using wave let transformer. It is gives high level security

IV. DESIGN

Encoding side:

- Message Encryption using RSA
- Message Embedded into Image using Twice bit-plane encoding.

Decoding side:

- Message Extraction
- Decryption Message

RSA Encryption:

The cryptographs depicts the simple concept that is: at the sender side, where the plaintext gets transformed into cipher textual content by the use of encryption algorithms, Cipher textual content is conveyed over the communicating channel and subsequently at the destination part the cipher textual content is transformed to the authentic plain textual content by using the use of decryption algorithm. It utilizes highly straightforward operations like growth and XOR expansion. The RSA algorithm is named after Ron Rivest, Adi Shamir and Len Adleman, who invented it in 1977. The basic technique was first discovered in 1973 by Clifford Cocks of CESG (part of the British GCHQ) but this was a secret until 1997. The patent taken out by RSA Labs has expired. The RSA cryptosystem is the most widely-used public key cryptography algorithm in the world. It can be used to encrypt a message without the need to exchange a secret key separately. The RSA algorithm can be used for both public key encryption and digital signatures. Its security is based on the difficulty of factoring large integers. Party A can send an encrypted message to party B without any prior exchange of secret keys.

Twice bit-plane encoding:

Embedding points and embedding intensity for a code block.

- The wavelet coefficients greater than a given threshold are chosen as candidate embedding points.
- According to the rate-distortion optimization, the lowest bit-plane which keeps unabridged after bit stream truncation is determined as the lowest embed-allowed bit plane of the code block.
- The embedding points and embedding intensity are adjusted adaptively on the basis of redundancy evaluation.

Scrambled synchronization:

Scrambled synchronization information and secret messages are embedded into the selected embedding points from the lowest embed-allowed bit-plane to higher ones. The synchronization information structure and the scrambling measure.

Rate-distortion optimization:

By doing this, messages are embedded into bit-planes that would not be truncated by rate-distortion optimization. The integrality of the embedded message is ensured at the cost of increased computational complexity and slightly changed compression ratio. The twice bit-plane encoding procedure is explained to execute the bit-plane encoding twice.

Message extraction:

First, the lowest bit-plane with complete information of all its three coding passes can be determined easily in the procedure of entropy decoding. Then the embedding points and their intensity are determined by the method similar to the encoder. Finally, both synchronization information and secret messages are extracted.

V. INPUT DESIGN

The input design is the link between the information system and the user. It comprises the developing specification and procedures for data preparation and those steps are necessary to put transaction data in to a usable form for processing can be achieved by inspecting the computer to read data from a written or printed document or it can occur by having people keying the data directly into the system. The design of input focuses on controlling the amount of input required, controlling the errors, avoiding delay, avoiding extra steps and keeping the process simple. The input is designed in such a way so that it provides

security and ease of use with retaining the privacy. Input Design considered the following things:'

- What data should be given as input?
- How the data should be arranged or coded?
- The dialog to guide the operating personnel in providing input.
- Methods for preparing input validations and steps to follow when error occur.

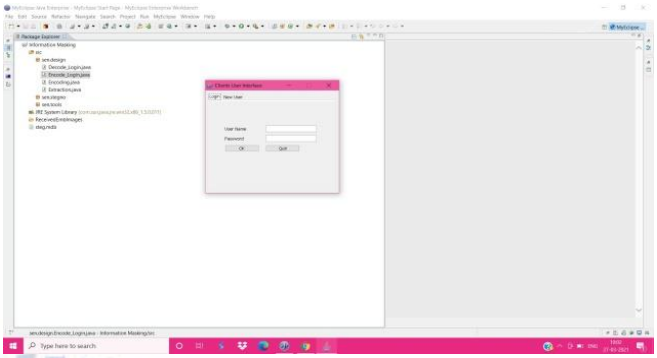
VI. OUTPUT DESIGN

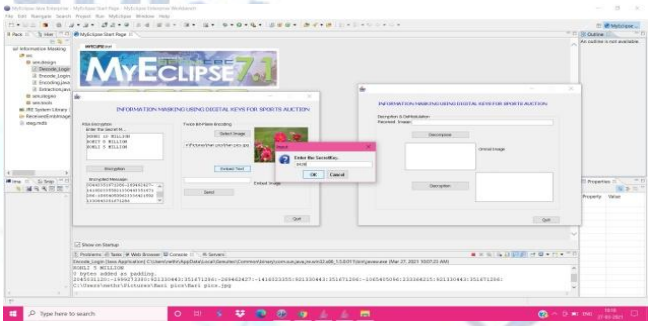
A quality output is one, which meets the requirements of the end user and presents the information clearly. In any system results of processing are communicated to the users and to other system through outputs. In output design it is determined how the information is to be displaced for immediate need and also the hard copy output. It is the most important and direct source information to the user. Efficient and intelligent output design improves the system's relationship to help user decision-making.

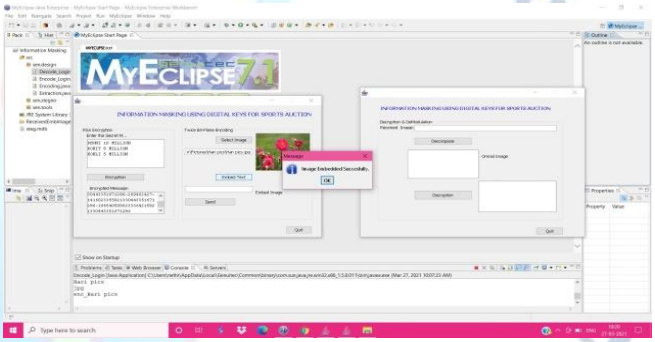
1. Designing computer output should proceed in an organized, well thought out manner; the right output must be developed while ensuring that each output element is designed so that people will find the system can use easily and effectively. When analysis design computer output, they should Identify the specific output that is needed to meet the requirements.
2. Select methods for presenting information.
3. Create document, report, or other formats that contain information produced by the system.

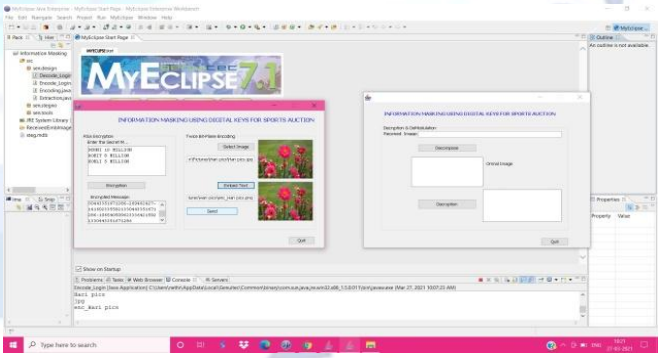
The output form of an information system should accomplish one or more of the following objectives.

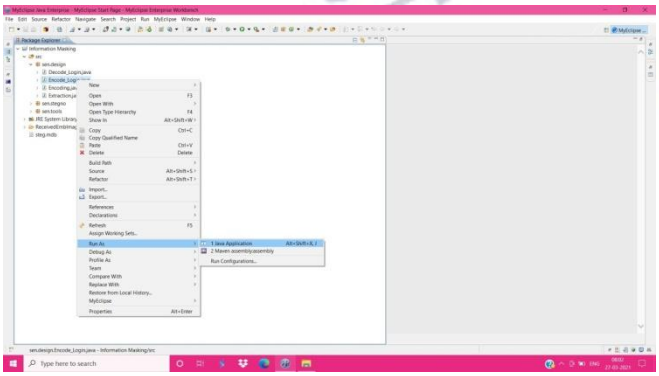
- Convey information about past activities, current status or projections of the Future.
- Signal important events, opportunities, problems, or warnings.
- Trigger an action.
- Confirm an action.

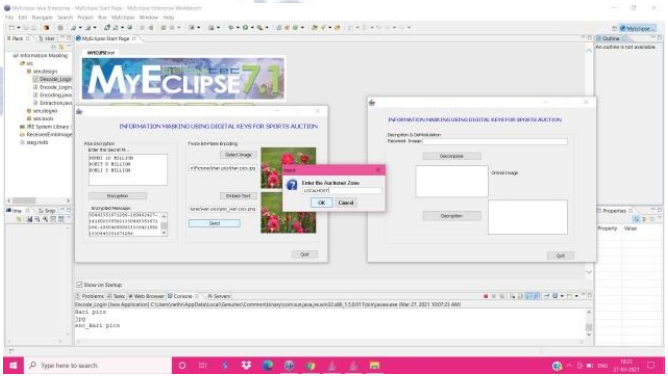


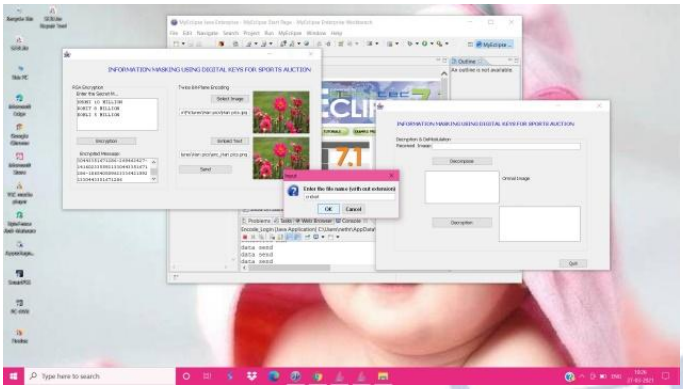


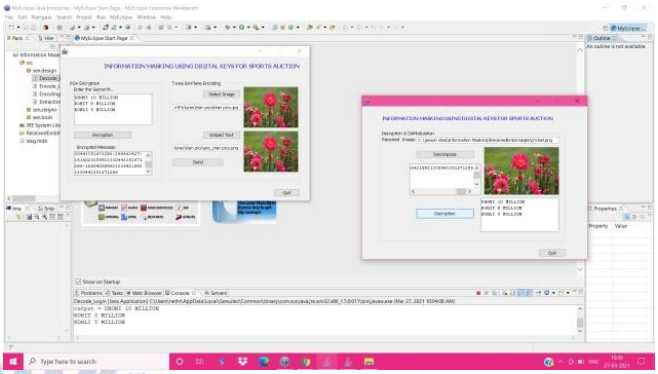


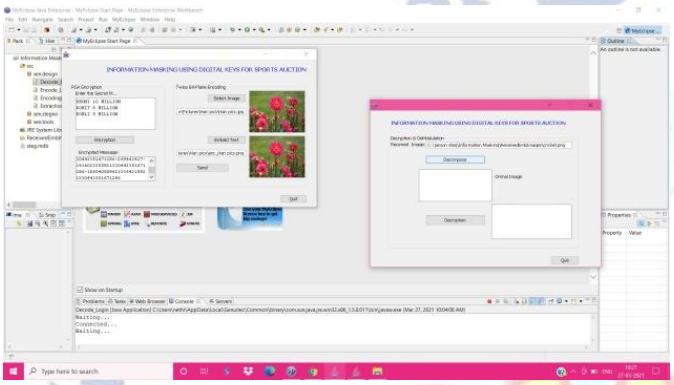


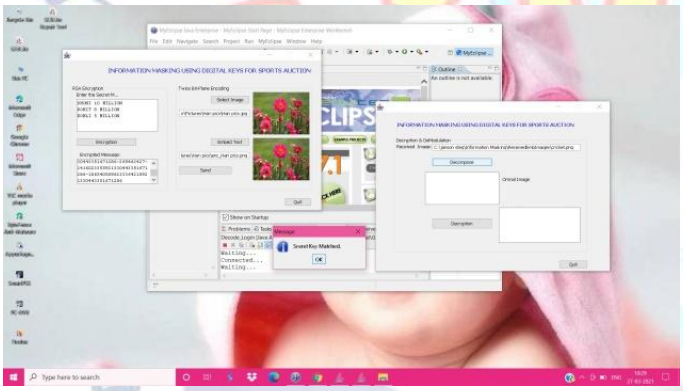


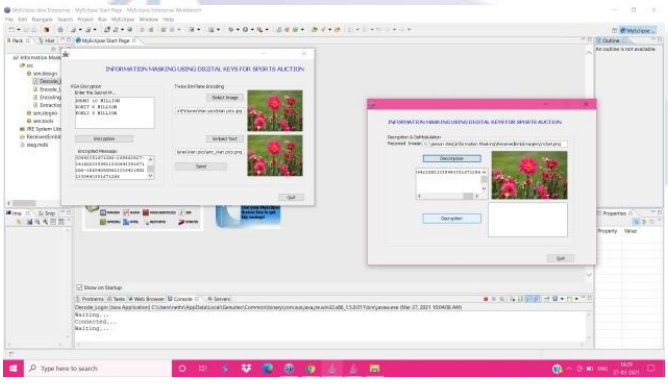












VII. CONCLUSION

Information masking using digital keys for image steganography has been implemented. An efficient steganography method for embedding secret messages into cover images without producing any major changes has been accomplished through bit plane encoding method. This technique alsoapplies a cryptographic method i.e. RSA algorithm to secure the secret message so that it is not easy to break the encryption without the key.

RSA algorithm itself is very secure that's why we used in this technique to increase the security of the secret message. A specified embedding technique uses hash function and also provide encryption of data uses RSA algorithm; makes our technique a very much usable and trustworthy to send information over any unsecure channel or internet.

This technique have been applied to.jpeg images; however it can work with any other formats with minor procedural modification like for compressed images. Performance analysis of the developed technique have been evaluated successfully.

VIII. SCOPE FOR FUTHURE ENHANCEMENT

The future scope for the proposed method might be the development of an enhanced steganography that can have the biometric authentication module along with encryption and decryption. Meanwhile the work can be enhanced for other data files like video, audio, text. Similarly the steganography technique can be developed for 3D images. The further work may contain combination of this method to message digesting algorithms.

REFERENCES

[1] M. Asikuzzaman and M. R. Pickering, "An overview of digital video watermarking," IEEE Trans. Circuits Syst. Video Technol., vol. 28, no. 9, pp. 2131–2153, 2018.

[2] M. Asikuzzaman, M. J. Alam, A. J. Lambert, and M. R. Pickering, "Imperceptible and robust blind video watermarking using chrominance embedding: A set of

approaches in the DT CWT domain," IEEE Trans. Inf. Forensics Security, vol. 9, no. 9, pp. 1502–1517, 2014.
[3] M. Asikuzzaman, M. J. Alam, A. J. Lambert, and M. R. Pickering, "Robust DT CWT-based DIBR 3D video watermarking using chrominance embedding," IEEE Trans. Multimedia, vol. 18, no. 9, pp. 1733–1748, 2016.
[4] J. Fridrich, Steganography in digital media: principles, algorithms, and applications. Cambridge University Press, 2009.
[5] T.-Y. Liu and W.-H. Tsai, "A new steganographic method for data hiding in microsoft word documents by a change tracking technique," IEEE Trans. Inf. Forensics Security, vol. 2, no. 1, pp. 24–30, 2007.
[6] B. Li, S. Tan, M. Wang, and J. Huang, "Investigation on cost assignment in spatial image steganography," IEEE Trans. Inf. Forensics Security, vol. 9, no. 8, pp. 1264–1277, 2014.
[7] C. Qin, C. C. Chang, Y. H. Huang, and L. T. Liao, "An inpaintingassisted reversible steganographic scheme using a histogram shifting mechanism," IEEE Trans. Circuits Syst. Video Technol., vol. 23, no. 7, pp. 1109–1118, 2013.
[8] Y. Huang, C. Liu, S. Tang, and S. Bai, "Steganography integration into a low-bit rate speech codec," IEEE Trans. Inf. Forensics Security, vol. 7, no. 6, pp. 1865–1875, 2012.
[9] D. Xu, R. Wang, and Y. Q. Shi, "Data hiding in encrypted H.264/AVC video streams by codeword substitution," IEEE Trans. Inf. Forensics Security, vol. 9, no. 4, pp. 596–606, 2014.
[10] S. Li and X. Zhang, "Towards construction based data hiding: From secrets to fingerprint images," IEEE Transactions on Image Processing, doi:10.1109/TIP.2018.2878290.
[11] B.-S. Kim, J.-G.Choi, and K.-H. Park, ``RST-resistant image watermarking using invariant centroid and reordered Fourier-Mellin transform,'' in Proc. Int. Workshop Digit. Watermarking, 2003, pp. 370-381.
[12] Z. Lin, L. Niu, and X. Jiang, ``A method on digital watermarking image against geometric distortion,'' in Proc. Int. Congr. Image Signal Process., Oct. 2015, pp. 130-134.
[13] M. Zareian and H. R. Tohidypour, ``A novel gain invariant quantization based watermarking approach,'' IEEE Trans. Inf. Forensics Security, vol. 9, no. 11, pp. 1804-1813, Nov. 2014.
[14] H. S. Kim and H.-K. Lee, ``Invariant image watermark using Zernike moments,'' IEEE Trans. Circuits Syst. Video Technol., vol. 13, no. 8, pp. 766-775, Aug. 2003.
[15] Y. Xin, S. Liao, and M. Pawlak, ``A multibit geometrically robust image watermark based on Zernike moments,'' in Proc. 17th Int. Conf. Pattern Recognit., Aug. 2004, pp. 861864.
[16] Y. Zhang, X. Luo, C. Yang, D. Ye, and F. Liu, ``A JPEG-compression resistant adaptive steganography based on relative relationship between DCT coeffcients,'' in Proc. Int. Conf. Availability Rel. Secur., Aug. 2015, pp. 461-466.