# EMBEDDED IMAGES AND TEXT FOR SECURITY

**D. SARITHA,** Assistant Professor, Dept. of Master of Computer Applications, Narayana Engineering College(Autonomous), Gudur.SPSR Nellore, AP
**I. SAHITHI,** PG Scholar, Dept. of Master of Computer Applications, Narayana Engineering College(Autonomous), Gudur.SPSR Nellore, AP

**Abstract_** An innovative reversible image data hiding scheme is presented in this paper. Encryption keys do not need to be known to achieve data embedding. SVM classifiers are used on the decoder side to distinguish between encrypted and non-encrypted image patches, allowing us to decode both the embedded message and original image signal simultaneously. It has a higher embedding capacity than existing methods and is able to reconstruct both the original image and embedded message perfectly. Our scheme's superior performance is supported by extensive experimental results. enlargement (PEE)-based techniques have been proven to be capable to provide the today's capacity-distortion overall performance [6[7][8].

Recently, the lookup on sign processing over encrypted area has received growing attention, specifically pushed via the wishes from Cloud computing structures and a number of privacy-preserving functions [11]–[14]. This has prompted the investigation of embedding extra records in the encrypted snap shots in a reversible fashion. In many sensible scenarios, e.g., impenetrable far off sensing and Cloud computing, the events who system the photo facts are un-trusted. To guard the privateness and security, all snap shots will be encrypted earlier than being forwarded to a un-trusted 1/3 birthday party for in addition processing. For instance, in tightly closed far off sensing, the satellite tv for pc images, upon being captured by way of on-board cameras, are encrypted and then despatched to the base station(s), as illustrated in Fig. 1. After receiving the encrypted images, the base station embeds a personal message, e.g., base station ID, vicinity information, time of arrival (TOA), nearby temperature, wind speed, etc., into the encrypted images. Eventually, the encrypted picture carrying the extra message is transmitted over a public community to a facts core for in addition investigation and storage. For protection reasons, any base station has no privilege of having access to the secret encryption key K pre-negotiated between the satellite tv for pc and the information center. This implies that the message embedding operations have to be carried out absolutely over the encrypted domain. In addition, comparable to the case of Cloud computing, it is virtually very high priced to enforce a dependable key management gadget (KMS) in such multi-party surroundings over insecure public networks, due to the variations in possession and manage of underlying infrastructures on which the KMS and the included assets are positioned [15] 1. It is consequently plenty preferred if impenetrable statistics hiding may want to be finished barring an extra secret statistics hiding key shared between the base station and the information center. Also, we respect easy embed-ding algorithm as the base station generally is limited by way of confined computing abilities and/or power. Finally, the records center, which has ample computing resources, extracts the embedded message and recovers the unique photo by using the use of the encryption key K.

In this work, we advocate an encrypted-domain RIDH scheme by means of especially taking the above-mentioned sketch preferences into consideration. The proposed method em-beds message thru a public key modulation mechanism, and performs records extraction via exploiting the statistical distinguish ability of encrypted and non-encrypted photo blocks. Since the decoding of the message bits and the authentic photo is tied together, our proposed method belongs to the category of non-separable RIDH options [16] two Compared with the state-of-the-arts, the proposed strategy gives greater embedding capacity, and is capable to gain perfect reconstruction of the unique photograph as nicely as the embedded message bits. Extensive experimental effects on a hundred check snap shots validate the most useful overall performance of our scheme.

## 2. PROPOSED WORK

1. In this work, we advocate an encrypted-domain RIDH scheme via in particular taking the above-mentioned layout preferences into consideration. The proposed approach embeds message thru a public key modulation mechanism, and performs records extraction through exploiting the statistical distinguishability of encrypted and non-encrypted photo blocks.
2. Since the decoding of the message bits and the unique photograph is tied together, our proposed approach belongs to the class of non-separable RIDH solutions
3. Compared with the state-of-the-arts, the proposed strategy presents greater embedding capacity, and is in a position to gain ideal reconstruction of the unique photo as properly as the embedded message bits.
4. Extensive experimental effects on take a look at pics validate the foremost overall performance of our scheme.

### 2.1 IMPLEMENTATION

**RIDH:**

Reversible image data hiding (RIDH) is a special category of data hiding technique, which ensures perfect reconstruction of the cover image upon the extraction of the embedded message. The reversibility makes such image data hiding approach particularly attractive in the critical scenarios, e.g., military and remote sensing, medical images sharing, law forensics and copyright authentication, where high fidelity of the reconstructed cover image is required.

**Discriminating Encrypted and Non-Encrypted Image Blocks:**

Compared with the original, un-encrypted block, the pixels in the encrypted block tend to have a much more uniform distribution. This motivates us to introduce the local entropy into the feature vector to capture such distinctive characteristics. However, we need to be cautious when calculating the entropy values because the number of available samples in a block would be quite limited, resulting in estimation bias, especially when the block size is small. For instance, in the case that M = N = 8, we only have 64 pixel samples, while the range of each sample is from 0 to 255. To reduce the negative effect of insufficient number of samples relative to the large range of each sample, we propose to compute the entropy quantity based on quantized samples, where the quantization step size is designed in accordance with the block size.

**Joint Data Extraction and Data Decryption:**

The decoder in the data center has the decryption key K, and attempts to recover both the embedded message and the original image simultaneously from [[f ]]w, which is assumed to be perfectly received without any distortions. Note that this assumption is made in almost all the existing RIDH methods. The joint data extraction and image decryption now becomes a blind signal separation problem as both Wi and fi are unknowns. Our strategy of solving this problem is based on the following observation: fi, as the original image block, very likely exhibits certain image structure, conveying sematic information. Note that Q[Wi]d must match one of the elements in Q = {Q0,Q1, • • • ,QS−1}. Then if we XOR fw i with all Qj 's, one of the results must be fi, which would demonstrate structural information. As will become clear shortly, the other results correspond to randomized blocks, which can be distinguished from the original, structured fi.

## 3.RESULTS AND DISCUSSIONS

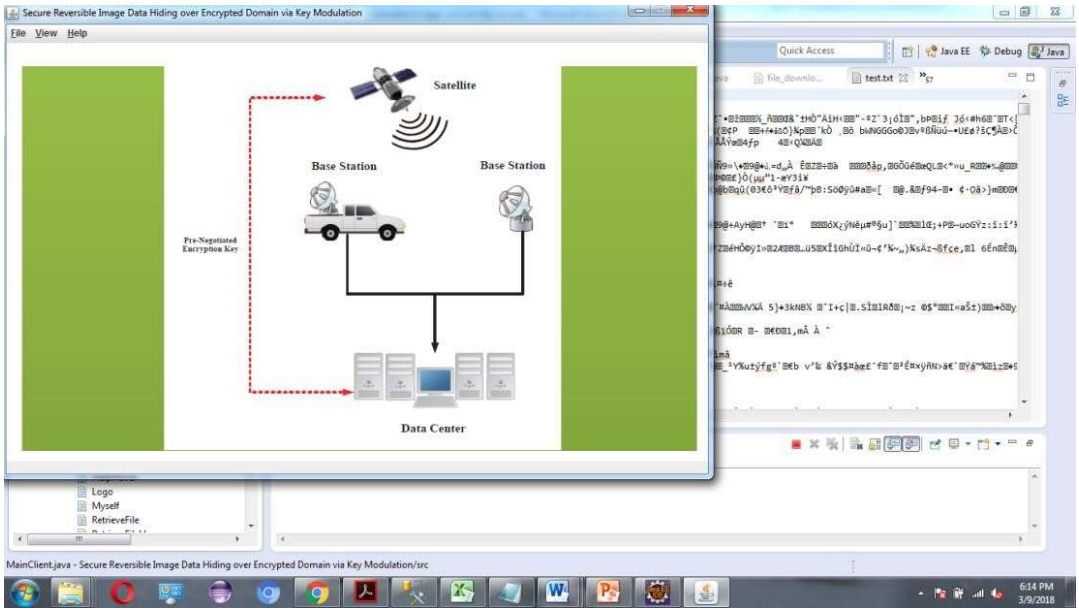


**Fig_3.1 Home Page**

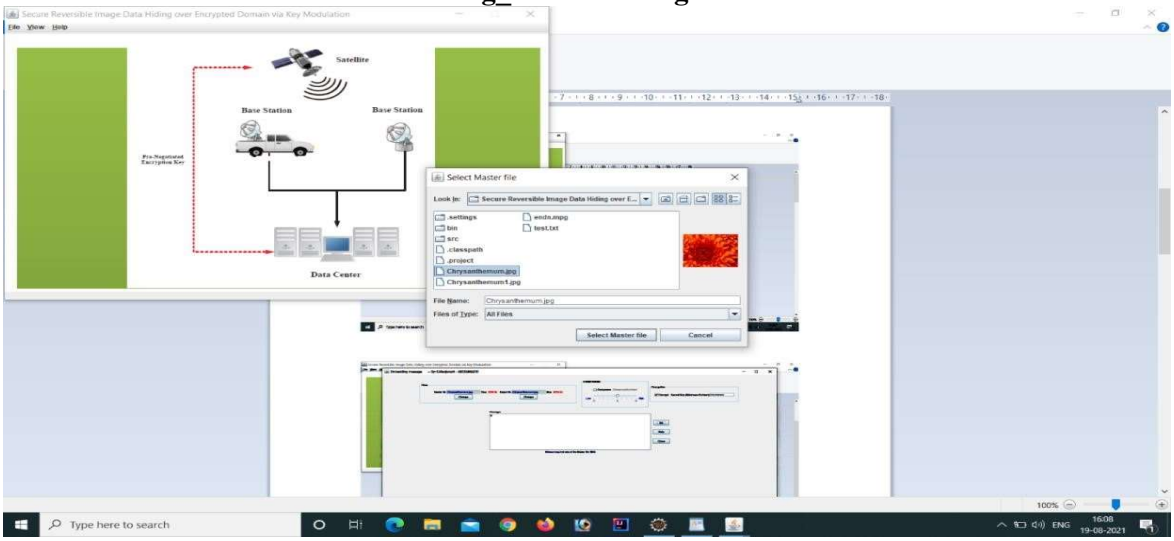


**Fig_3.2 Uploading File Page**

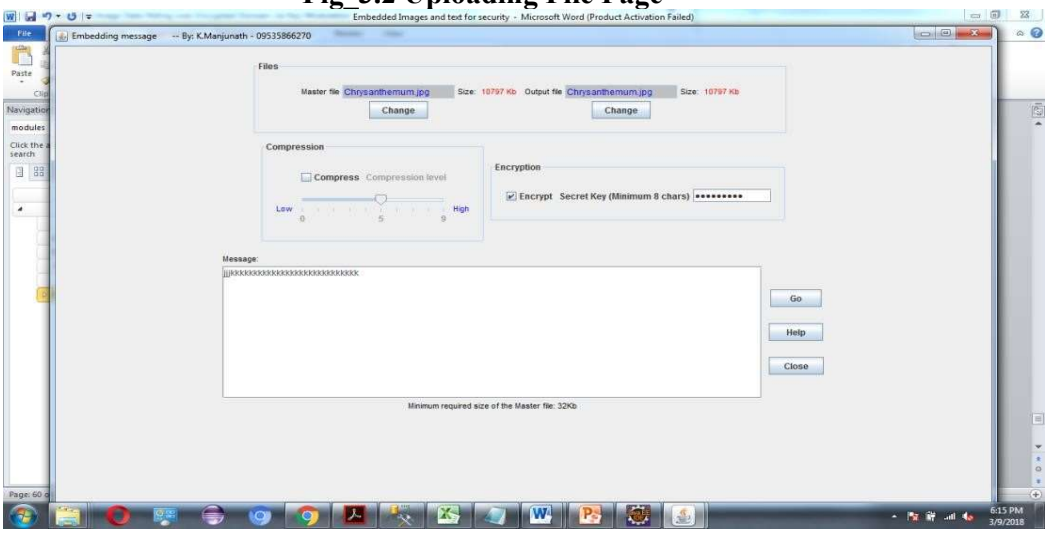


**Fig_3.3 Message Page**

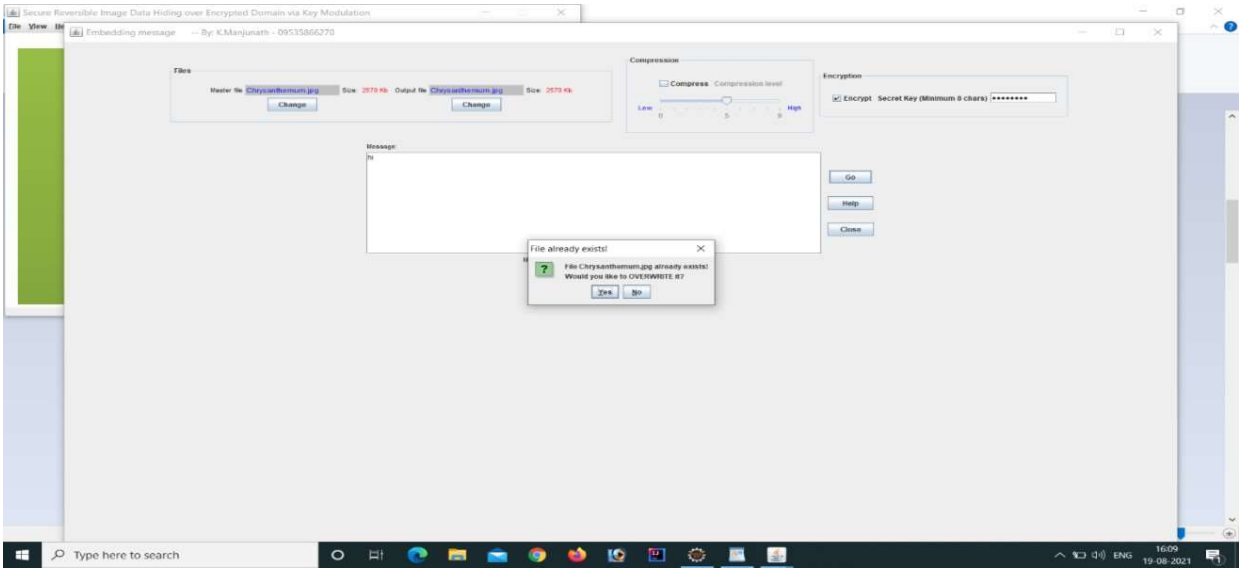


**Fig_3.4 Text File Encrypted Page**

## 4.CONCLUSION

Using an encrypted domain, we propose a secure reversible image data hiding scheme (RIDH). It is proposed that data be embedded using a public key modulation mechanism, which does not require access to the secret encryption key. A powerful two-class SVM classifier will be used to discriminate encrypted and non-encrypted image patches, allowing us to decode both the embedded message and the original image signal perfectly together. Our proposed RIDH method has also been extensively tested in encrypted domains.

## 5.REFERENCES

1.M. U. Celik, G. Sharma, A. M. Tekalp, E. Saber, "Lossless generalized-LSB data embedding", ***IEEE Trans. Image Process.***, vol. 14, no. 2, pp. 253-6, Feb. 2005.

2.M. U. Celik, G. Sharma, A. M. Tekalp, "Lossless watermarking for image authentication: A new framework and an implementation", ***IEEE Trans. Image Process.***, vol. 15, no. 4, pp. 1042-1049, Apr. 2006.

3.Z. Ni, Y.-Q. Shi, N. Ansari, W. Su, "Reversible data hiding", ***IEEE Trans. Circuits Syst. Video Technol.***, vol. 16, no. 3, pp. 354-362, Mar. 2006.

4.X. Li, W. Zhang, X. Gui, B. Yang, "A novel reversible data hiding scheme based on two-dimensional difference-histogram modification", ***IEEE Trans. Inf. Forensics Security***, vol. 8, no. 7, pp. 1091-1100, Jul. 2013.

5.C. Qin, C.-C. Chang, Y.-H. Huang, L.-T. Liao, "An inpainting-assisted reversible steganographic scheme using a histogram shifting mechanism", ***IEEE Trans. Circuits Syst. Video Technol.***, vol. 23, no. 7, pp. 1109-1118, Jul. 2013.

6.W.-L. Tai, C.-M. Yeh, C.-C. Chang, "Reversible data hiding based on histogram modification of pixel differences", ***IEEE Trans. Circuits Syst. Video Technol.***, vol.
19, no. 6, pp. 906-910, Jun. 2009.

7.J. Tian, "Reversible data embedding using a difference expansion", ***IEEE Trans. Circuits Syst. Video Technol.***, vol. 13, no. 8, pp. 890-896, Aug. 20.

8.V. Sucharita,S. Jyoti An Identification of Penaeid Prawn Species Based on Histogram Values, ,Volume 3, Issue 7, July 2013 ISSN: 2277 128X