

Enhanced Text and Image Cryptography using Watermarking for Password Privacy

K. N. V Suresh Varma, K. N. V Satyanarana, B. Lakshmi Sai Tulasi,
Bh. M. L Harshitha, A. C. L. Ramterdh, A. Sai Raj

Abstract: *This paper proposes a new method for password security and the password is encrypted and decrypted by using watermarking, Conventional password encryption method for user substantiation is to convert the password into hash values. These hash-based password methods are comparatively agile because those are dependent on text and renowned cryptography. However, those can be vulnerable to cyber-attacks by hash-based cracking tool. Attackers can rigorously totalize an original password from hash value when that is comparatively simple and modest. Hence, many hacking contretemps have been occurred consistently in systems endorsing those hash-based schemes. Contrasting from the conventional methods based on hash and text we propose Enhanced text and image cryptography using watermarking method. The user chooses source image, output image, information which is text or image is to be hidden along with security key. The information given by user is hidden in source image by water marking process that includes Cipher text and public channel. To retrieve the hidden information the decrypted key is used which is same as the encrypted key. Hence information which is text or image is recovered without any loss.*

Key words: cryptography, watermarking, image hiding, encryption and decryption.

I. INTRODUCTION

Watermarking offers the elaborate info regarding strategies and technologies that conceal info, as an example variety or text, in digital media, like pictures, audio or video. The embedding occurred by handling the content of the digital information, which suggests {the information the knowledge the information} isn't embedded within the frame round the data. The conceal method needs to be such the alterations of the media are undetectable. For images, this suggests that the alterations of the element values have to be compelled to be unseen. Moreover, the watermark should be either sturdy or fragile, hard on the applying. By "robust", we have a tendency to mean the competency of the watermark to face up to alterations of the media, like lossy compression (where pressing information and so pressing it retrieves information which will somewhat be completely different from the first, however is contiguous enough to be helpful in some way), scaling, and cropping, among others. Pictures assume an

Revised Manuscript Received on June 01, 2019.

K.N.V Suresh varma, Department of Electronics and Communication , SRKR Engineering College, Bhimavaram, India
K. N. V Satyanarayana, Department of Electronics and Communication , SRKR Engineering College, Bhimavaram, India
B. Lakshmi Sai Tulasi, Department of Electronics and Communication, SRKR Engineering College, Bhimavaram, India
Bh. M. L Harshitha, Department of Electronics and Communication, SRKR Engineering College, Bhimavaram, India
A.C.L. Ramteerdh, Department of Electronics and Communication, SRKR Engineering College, Bhimavaram, India
A.Sai Raj, Department of Electronics and Communication, SRKR Engineering College, Bhimavaram, India

essential part in a few applications like remote detecting, biomedical, video conferencing. Enthusiasm for advanced picture preparing techniques originates from the accompanying foremost application ranges: change of pictorial data for human elucidation; and handling of picture information for capacity and transmission for machine recognition. At whatever point a picture must be transmitted, two critical issues should be tended to. One is to suit the picture inside the assigned data transfer capacity and the other is to guarantee secure transmission of pictures. Picture pressure and picture encryption are two crucial picture preparing methods broadly utilized towards meeting the necessity of proficient use of data transfer capacity and security. Scrambling the picture by following specific advances which includes changing the picture puts as it were. These procedure may include techniques like Scrambling, Chaotic Mapping, Inversion. These Process can be taken after with set of keys which can choose the request of these calculation that could be taken after for encryption. As pixels stays in the picture itself, it might be defenseless against assault of grave expert assaults yet utilizing variable length. Picture Encryption implies changing proselyte the picture into garbled configuration.

II. METHODOLOGY

MATLAB stands for MATrix LABoratory and also the software system is made up around vectors and matrices. The MATLAB application is made round the MATLAB scripting language. Common usage of the MATLAB application involves exploitation the Command Window as associate degree interactive mathematical shell or execution text files containing MATLAB code. MATLAB supports developing applications with graphical program (GUI) options. MATLAB includes GUIDE [23] (GUI development environment) for diagrammatically coming up with GUIs. It additionally has tightly integrated graph-plotting options. MATLAB may be a proprietary product of MathWorks, therefore users are subject to marketer lock-in. Though MATLAB Builder product will deploy MATLAB functions as library files which may be used with .NET or Java application building atmosphere, future development can still be tied to the MATLAB language.



III. OBJECTIVE

Advanced watermarking is that the demonstration of hiding a message related with a computerized flag (for example a picture, melody, and video) at interims the flag itself. it's an idea intently connected with steganography, in that they each conceal a message inside an advanced flag. Be that as it may, what isolates them is their objective. Watermarking attempts to cover a message related with the specific substance of the computerized flag, though in steganography the advanced flag has no significance the message, and it's basically utilized as a shade to cover its reality. Watermarking has been around for a long time, inside the assortment of watermarks discovered abdominal muscle initio in plain paper and later on in paper bills. Nonetheless, the segment of computerized watermarking was exclusively created all through the most recent fifteen years and it's as of now getting utilized for a few very surprising applications. a fresh out of the plastic new watermarking topic can created to installed message comparatively as picture into the main picture. The arranged subject upheld bit framework with encoding calculations. Furthermore, invert technique for extraction the content and picture from the watermarked picture is referenced, when separate the content string and picture contrasted and unique picture.

IV. CRYPTOGRAPHY:

Cryptography is that the method of changing plaintext into Ciphertext. Cipher: the algorithmic rule that will the encoding. Ciphertext the encrypted (scrambled) version of the message. Message altered to be undecipherable by anyone except the supposed recipients. The technique accustomed modification over the primary data into mystery code or data is termed data encoding procedure for a good vary of data. In this project, we have a tendency to consider Image encoding that has applications in internet correspondence, media frameworks, restorative imaging, telemedicine, military correspondence; and then on. footage encoding is exclusive in respect to the simple data encoding. therefore as a rule the knowledge stowage away in image includes four stages. 1. selection of the mystery media wherever the knowledge are going to be lined up. 2. The covert message or knowledge that ought to are veiled in the duvet image. 3. A capability which will be used to hide {the data the knowledge the data} within the cowl media and its backwards to recover the shrouded information. 4. A discretionary key or the key word to verify or to hide out and unhide the information.

Grouping According to Keys :

By and large, there are two sorts of cryptosystems:

- (1) Symmetric (private) key cryptography.
- (2) Asymmetric (open) key cryptography.

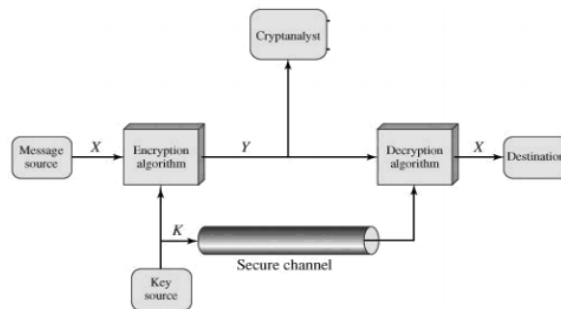


Fig 1: Symmetric Key Cryptography Encryption Model

In Fig 1, the sender scrambles the information (plain content) utilizing the encryption key and the recipient unscrambles the encoded information (figure picture) into the first information (plain picture) utilizing the decoding key. In symmetric encryption, both encryption and unscrambling keys are indistinguishable.

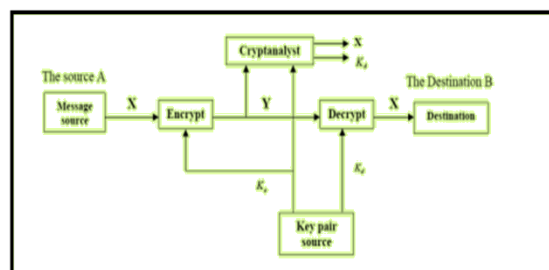


Fig 2 : Asymmetric Key Cryptography

In Fig 2 demonstrates the general population key encryption (hilter kilter encryption), in which the encryption and unscrambling keys are extraordinary. Rather than one key, there are two distinctive keys; an open () and a private (). Open key cryptography tackles the issue of regular cryptosystems by dispersing the key.

V. IMAGE CONTENTS

The three pictures in the figure 3 are of a similar size, i.e., 512 lines and 512 segments, meant by 512×512, for an aggregate of 262144 pixels. The pixel esteems in a double picture as appeared in figure are any two esteems when all is said in done that are standardized, e.g., 0 and 1 or 0 and 255 Fig (a) is the binary image .The pixel esteems in a grayscale picture as in Figure (b) are whole number esteems in the vicinity of 0 and 255, which have an aggregate of 256 dark esteem portrayals. A multispectral picture regularly contains data outside the typical human perceptual range. A real nature picture as appeared in figure (c) contains three grayscale pictures as three parts: red, green, and blue alluding to below figure.





Fig 3 :Types Of Images

Image properties	Bits resolution	Colour space
Binary image (black and white)	1	2 colours
Gray scale (monochrome)	8	256 gray levels
Coloured image	8	256 colours
Coloured image	16	65536 colours
True colour (RGB)	24	16,777,216 colours

Table 1: Properties Of Images

Table 1 shows the picture shading space. As found in Table 1 the quantity of bits expands, the picture quality is additionally expanded. Notwithstanding, capacity necessities will increment, bringing about an immediate connection between the picture stockpiling size and the bits determination.

VI. IMAGE HIDING

Picture covering up can meet the prerequisites like security, impalpability, vigor, respectability. Picture stowing away here is refined through Multiplexing. Picture multiplexing is the way toward transmitting at least two pictures at the same time in a solitary channel which is accomplished by blending the pictures. Merging is a system by methods for which the pixel estimations of two separate pictures are mixed with the goal that the resultant picture is unimportant. Such pictures can't be recovered unless the request of scrambling is resolved. This is done so as to make picture transmission more secure. The base image or target image into that mystery image is to be coated up correct to own some likeness with mystery image. It ought to be potential by coordinating the h-values.

H esteem may be computed as takes when.

$$H(r', g', b') = b' + N b * r' + N b * Nr * g'$$

Algorithm for concealing :

Obtain the constituent values of each the pictures.

Merge the savings bank and LSB constituent to get 0.5 computer memory unit words.

These four bit values square measure then given as inputs to the delineated Compress secret writing formula.

The encrypted and compressed pixels square measure transmitted.

On reception the key's wont to retrieve the constituent values. The savings bank and LSB bits square measure re-arranged so as to get the first image.

WATER MARK ALGORITHMS FOR TEXT:

1. Peruse the info picture (im).
2. Peruse the content string (str).
3. Convert the info picture into single section.
4. Discover the length of string.
5. Check if the picture measure is adequate to oblige the string.
6. Apply bitand capacity to 0 the least critical piece of every component of picture.
7. Discover the rand permutation utilizing rand perm
8. Apply stage 9-11 for each sanction of the string (for key or without key) for each piece of each character.
9. Count of the file of the pixels to be altered.
10. Convert each contract into 8 bit framework at that point Apply bitget capacity to secure the j-th bit of the ith character.
11. Apply bitset capacity to set the pixel shown by file.
12. Embeddings a character top (end of string).
13. For each piece of the character top.
14. Computing the list, Updating bits into layout t_im.
15. Remake the watermarked picture

WATER MARK ALGORITHMS FOR IMAGE

1. Peruse the information (picture).
2. Peruse the logo for water stamping (im_logo).
3. Discover the measure of im_logo.Check if picture is sufficiently substantial to hold im_logo.
5. Convert the picture into a solitary segment vector.
6. Convert im_logo into a solitary segment vector.
7. Apply bitand work with picture.
8. Apply stage 9-11 for each piece of the every pixel.
9. Ascertaining the straight record of the pixel to be changed.
10. Apply bitget work for each piece of pixel.
11. Apply bitset for each file.
12. Embeddings a character top (end of string).
13. For each piece of the character top.
14. Ascertaining the record, Updating bits into format t_im.
15. Reproduce the watermarked picture.

DEWATERMARK ALGORITHMS

1. Peruse watermarked picture and key.
2. Convert the watermarked picture into single segment.
3. Apply randperm work for arbitrary factors.
4. Apply circle to discover the character top.
5. Utilizing file discover the bit position utilizing bitget work.
6. Concentrate the least huge piece.
7. Change blend of bit into character utilizing and store into bitword.
8. Show the separated picture or content

VII.COMPRESSION TOOL

Utilizing above proposed algorithms designed a tool in MATLAB and run on MATLAN command, interface is shown in the figure 5.



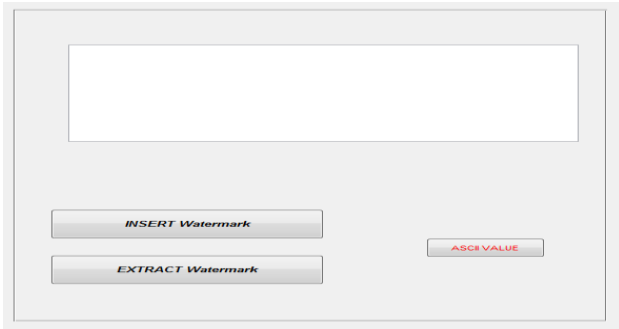


Fig 4 : Output Showing Window

VIII. WATER MARK INSERTION

Click on insert the water imprint the window show in fig 6 and first read the information picture and compose the test as a string and apply the said water mark calculations, results are appeared underneath for encryption key can be embedded however key ought to be recollect at the season of dewater stamping other we can't separate the water checked picture from the installed Image



Fig 7: Stego Image For Text Embedding

Image as water Mark:

In Fig 8 we read one info picture and one water mark picture and addition the water mark into the first picture, result are appear in beneath with image and after click on insert it shows the stego image for secrete image embedding is shown in fig 9.

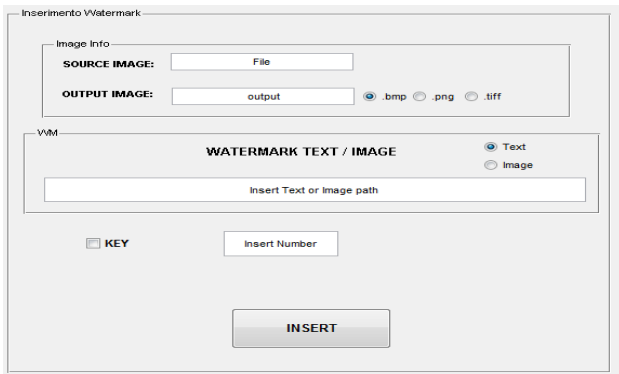


Fig 5: Insert Watermark Window

Text as water Mark:

In Fig 6 it shows the insert watermark window and it is used test as watermark and in this secret text embedding takes place. Fig 7 shows the after enter the insert watermark it shows the stego image for the text embedding.

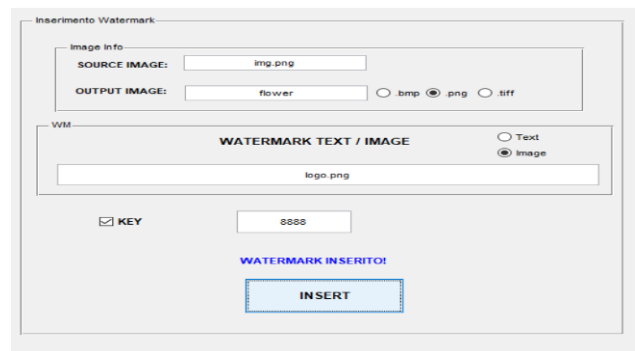


Fig 8: Secret Image Embedding

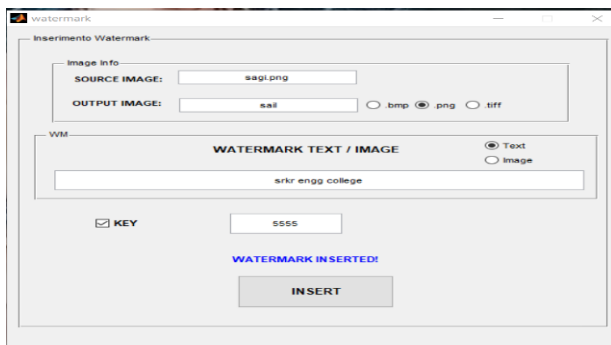


Fig 6: Secret Text Embedding

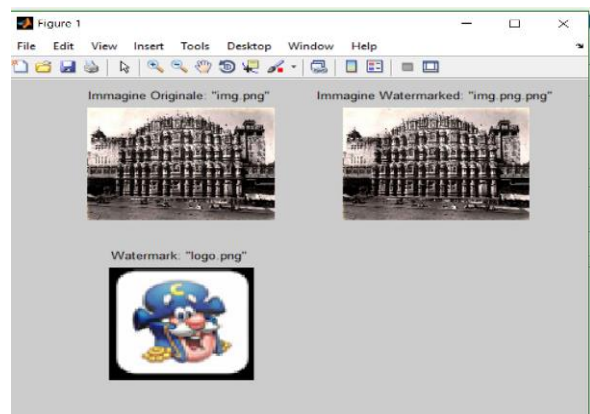


Fig 9: Stago Image For Image Embedding

IX. WATER MARK EXTRACTION:

Click on concentrate catch for concentrate the water mark picture from the implanted picture, read the implanted picture (encryption key which is embedded amid the inclusion procedure) and apply the said de water mark calculations, Fig 10 shows the window which extract the



watermark and embedded string show which is identical as information string and same as for image it shows in the Fig 11 results are appeared underneath.

Text extraction:

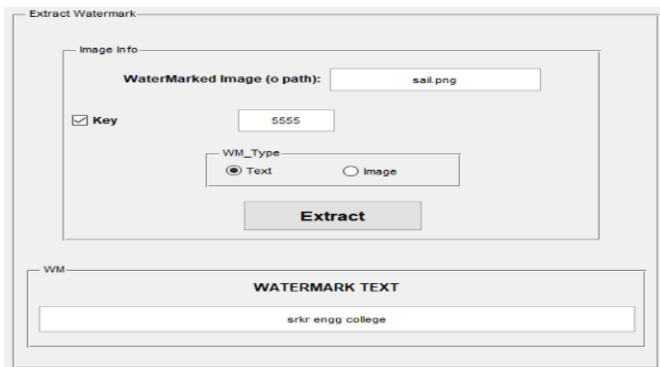


Fig 10: Hidden Text Extracting

Image extraction:

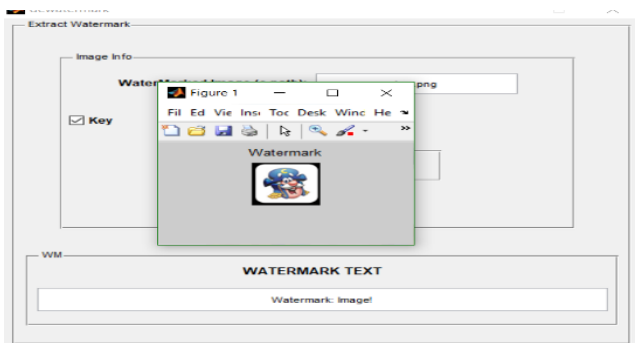


Fig 11: Hidden Image Extracting

X. CONCLUSION AND FUTURE SCOPE :

In this paper we have utilized the Encoding Technique on pictures to acquire secure picture. To enhance the measure of security and measure of encryption, the current picture encryption calculations are utilized to create half and half ideas for Image Encryption and Partial Image Encryption. Each proposed encryption methods are one of a kind in its temperament. Parallel to Gray code change idea in picture encryption is better helpful in the event of encryption of compacted picture and which prompts more pressure..

- [1] Quiet Information Security (regarding halfway picture encryption) in Tele-solution.
- [2] Motion/Posture based security in banking exchange.
- [3] Equipment - programming key for shrewd camera/advanced cells est.
- [4] Half and half multi layered - multi enter based security in military and satellite correspondence.
- [5] Architecture (FPGA/DSP) outline for Image Encryption Processor.
- [6] Gesture based key idea builds the security level, for this situation alongside a content key - hand signal are likewise used to give higher security .

REFERENCES:

- [1]. Zhengjun Liu, She Li, Wei Liu, Yanhua Wang, Shutian Liu, "Picture encryption calculation by utilizing fragmentary Fourier change and pixel scrambling operation in light of twofold irregular stage encoding", *Optics and Lasers in Engineering* 51 (2013) 8– 14.
- [2]. Nanrun Zhou, XingbinLiu, YeZhang, YixianYang, "Picture encryption conspire in light of fragmentary Mellin change and stage recovery method in partial Fourier space", *Optics and Laser Technology* 47 (2013) 341– 346.
- [3]. Guodong Ye, Kwok-wowong, "A picture encryption plot in view of time-delay and hyperchaotic framework", *Nonlinear Dyn* (2013) 259– 267.
- [4]. TheDucKieu, Zhi-Hui Wang, Chin-Chen Chang, and Ming-Chu Li, "A Sudoku Based Wet Paper Hiding Scheme", *International Journal of Smart Home*, 2009, 1-12.
- [5]. Jaw Chen Chang, Pei-Yu Lin, Zhi Hui Wang and Ming Chu Li, "A Sudoku-based Secret Image Sharing Scheme with Reversibility", *Journal Of Communications*, Vol. 5, No. 1, January 2010, 5-12.
- [6]. Roshan Shetty B R, Rohith J, Mukund V, Rohan Honwade, ShantaRangaswamy, "Universal Conference on Advances in Recent Technologies in Communication and Computing", 2009.
- [7]. Ante Poljicak, Lidija Mandic, Darko Agic, "Discrete Fourier transform-based watermarking method with an optimal implementation radius", *Journal of Electronic Imaging* 20(3), 033008 (Jul-Sep 2011).
- [8]. Ante Poljicak, Lidija Mandic, Darko Agic, "Discrete Fourier transform-based watermarking method with an optimal implementation radius", *Journal of Electronic Imaging* 20(3), 033008 (Jul-Sep 2011).
- [9]. L. N. Hu and L. G. Jiang, "Blind Detection of LSB Watermarking at Low Embedding Rate in Grayscale Images," In: M. Celik, G. Sharma, E. Saber and A. Tekalp, Eds., *Hierarchical Watermarking for secure Image Authentication with Localization*, IEEE Transactions on Image Process, Vol. 11, No. 6, 2002, pp. 585-595.
- [10]. N. F. Johnson, Z. Duric and S. Jajodia, "Information Hiding: Steganography and Watermarking—Attacks and Countermeasures," Kluwer Academic Press, Norwell, 2001,
- [11]. P. Wong, "A Watermark for Image Integrity and Ownership Verification," *Image Processing, Image Quality, Image Capture Systems Conference*, Portland, May 1998, pp. 374379.
- [12]. W. Puech and j.m. rodrigues, "a new cryptowatermarking method for medical images safe transfer".
- [13]. Jung-Hee Seo*, and Hung-Bog Park, "Data-Hiding Method using Digital Watermark in the Public Multimedia Network", *International Journal of Information Processing Systems*, Vol.2, No.2, June 2006.
- [14]. Siddhart Manay, Byung-Woo Hong, Anthony J. Yezzi, and Stefano Soatto Integral invariant signatures, In *Proceedings of ECCV 2004*, number LNCS 3024, pages 8799. Springer, 2004.
- [15]. Helmut Pottmann, Qixing Huang, Yongliang Yang, and Stefan KAolpl. Integral invariants for robust geometry processing, Technical report, *Geometry Preprint Series*, Vienna Univ. of Technology, 2005.

AUTHORS PROFILE



K.N.V Suresh varma, M.Tech, Asst. Professor Dept of Electronics and Communication, SRKR Engineering College, Bhimavaram, India



K.N.V Satyanarayana, M.Tech, Asst. Professor Dept of Electronics and Communication, SRKR Engineering College, Bhimavaram, India



B.Lakshmi Sai Tulasi, B.Tech, Electronics and Communication engineering, SRKR Engineering College, Bhimavaram, India



Bh. M. L. Harshitha, B.Tech , Electronics and Communication engineering, SRKR Engineering College, Bhimavaram, Indi



A.C .L. Ramteerdh, B.Tech , Electronics and Communication engineering , SRKR Engineering College, Bhimavaram, India



A Sai Raj, B.Tech , Electronics and Communication engineering , SRKR Engineering College, Bhimavaram, India