ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 7, July 2015

Enhance Security for Image Encryption and Decryption by Applying Hybrid Techniques Using MATLAB

Jai Singh[1], Kamil Hasan[2], Ravinder Kumar[3]

M.Tech Scholar, Dept. of ECE., AL-FALAH University, Faridabad, Haryana, India[1]

Assistant Professor, Dept. of ECE., AL-FALAH University, Faridabad, Haryana, India[2,3]

ABSTRACT: Cryptography, Steganography and Digital watermarking are widely used for Image Encryption and Textual Data Encryption and also we have various classification of these techniques. In this paper we study of Hybrid Cryptographic Encryption Techniques and also use of other encryption techniques to enhance their level of security and also study of their combination of Hybrid Techniques which is included of combination of cryptographic and Digital Watermarking Technique's.Hybrid approach for encryption gives more and strictly secured information, it's very difficult to find out anyhow any information, none of hacker easy to detect even truly they failed to decrypt information little bit.

KEYWORDS: Cryptography, Steganography, Digital Watermarking, Cipher, Image Encryption, Hybrid Techniques Decryption

I. INTRODUCTION

Security is a broad topic and covers a multitude of sins. In its simplest form, it is concerned with making sure that nosy people cannot read, or worse yet, secretly modify message intended for other recipients. It is concerned with people trying to access remote services that they are not authorized to use. For ensuring the security and privacy of the information that is being communicated, a process called data encryption is essential. Encryption is carried out at the sending end. In this, sender transform the original information to another form, and sends the transformed information. At the receiving end, an exactly opposite process called Decryption is called out in which the received information is transformed back to its original form. Encryption and Decryption are carried out by the presentation layer.

II. VARIOUS TECHNIQUES FOR ENCRYPTION

Well we have many more techniques for encryption but mainly we discuss about Steganography, Digital watermarking, Cryptography and their Hybrid combination encryption approaches.
Hybrid approach for encryption gives more and strictly secured information, it's very difficult to find out anyhow any information, none of hacker easy to detect even truly they failed to decrypt information little bit.

A. *Steganography*

The art and science of hiding information by embedding messages within other, seemingly harmless messages. Steganography works by replacing bits of useless or unused data in regular computer files (such as graphics, sound, text, HTML, or even floppy disk) with bits of different, invisible information. This hidden information can be plain text, cipher text, or even images.

Steganography sometimes is used when encryption is not permitted. Or, more commonly, steganography is used to supplement encryption. An encrypted file may still hide information using steganography, so even if the encrypted file is deciphered, the hidden message is not seen.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 7, July 2015

Steganography (literally meaning covered writing) dates back to ancient Greece, where common practices consisted of etching messages in wooden tablets and covering them with wax, and tattooing a shaved messenger's head, letting his hair grow back, then shaving it again when he arrived at his contact point.

B. *Digital Watermarking for image/video Encryption*
Embedding a hidden stream of bits in a file is called Digital Watermarking. The file could be an image, audio, video or text. A digital watermark is a kind of marker covertly embedded in a noise-tolerant signal such as an audio, video or image data. It is typically used to identify ownership of the copyright of such signal. Nowadays, digital watermarking has many applications such as broadcast monitoring, owner identification, proof of ownership, transaction tracking, content authentication, copy control, device control, and file reconstruction (Cox et. al., 2008). In literature, the host file is called the "asset", and the bit stream is called the "message". The main specifications of a watermarking system are: Robustness (Against intentional attacks or unintentional ones such as compression), Imperceptibility, and Capacity. Importance of each depends on the application. As a matter of fact there is a trade-off between these factors (Barni & Bartolini, 2004). Although watermarking in some literature includes visible imprints, here we only mean the invisible embedding of the data.

2D, 3D, 4D data we can secure by using Digital Watermarking which is very best techniques over Steganography.Digital watermarking relates to a technology known as steganography, which literally means "covered writing." It is a technique designed to secure a message by hiding that message within another object so that it can be kept secret from everyone except the intended recipient. This is quite different from cryptography that renders the message (which is typically visible or audible) unintelligible to unauthorized viewers to prevent access.
Steganographic messages may or may not be encrypted. Through many advances in the technology, steganography is now successfully used across a variety of industries. Digital watermarks provide the means of hiding steganographic messages for many different purposes.

Digital watermarking provides an added layer of security to the content protection chain to deter unauthorized use of content by embedding watermarks that identify the permitted uses of the content into the music or motion picture soundtrack prior to theatrical, packaged media (Blu-ray Discs, DVDs) and online digital distribution. Devices read the watermark during playback or copying of content. If the watermark indicates that the use is unauthorized, the playback or copying is stopped or the audio is muted, and an explanatory message may be displayed.

Effective content protection helps content owners:-

- Protect audio, film and video entertainment content throughout all release windows.
- Communicate copyright ownership and usage rights of their content.
- Protect content against common threats of piracy including camcorder recording, peer-to-peer file sharing, copying, format conversion, encoding and other forms of re-processing.
- Ensure content is protected through multiple packaged media and digital file formats.
- Secure content without impacting the consumer entertainment experience.

C. *Cryptography*
Cryptography Research is committed to helping industries fight fraud, piracy, counterfeiting, and other forms of abuse. Our research, technology, and services help solve many of the world's most difficult data security problems.

Cryptography is the science of using mathematics to encrypt and decrypt information. Once the information has been encrypted, it can be stored on insecure media or transmitted on an insecure network (like the Internet) so that it cannot be read by anyone except the intended recipient.

Encryption is the process in which data (plaintext) is translated into something that appears to be random and meaningless (ciphertext). Decryption is the process in which the ciphertext is converted back to plaintext.

A cryptographic algorithm, or cipher, is a mathematical function used in the encryption and decryption process. A cryptographic algorithm works in combination with a key (a number, word, or phrase) to encrypt and decrypt data. To

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 7, July 2015

encrypt, the algorithm mathematically combines the information to be protected with a supplied key. The result of this combination is the encrypted data. To decrypt, the algorithm performs a calculation combining the encrypted data with a supplied key. The result of this combination is the decrypted data. If either the key or the data is modified, the algorithm produces a different result. The goal of every encryption algorithm is to make it as difficult as possible to decrypt the generated ciphertext without using the key. If a really good encryption algorithm is used, then there is no technique significantly better than methodically trying every possible key. Even for a key size of just 40 bits, this works out to 2ˆ40 (just over 1 trillion) possible keys.

III. HYBRID TECHNIQUES APPLIED WITH COMBINATION OF CRYPTOGRAPHIC AND DIGITAL WATERMARKING

Firstly we applied Digital Watermarking on image and then we also apply a cryptographic techniques. We have many different ways or classification of Digital Watermarking and Cryptography and further we will also try to do same Hybrid Process with steganography.

Let's start with steps and simulation on Matlab how to apply Digital Watermarking on image. We have many ways but we try to secure image via two way which next to show in few figures and also all steps mentioned with few lines of code.

Algorithm for Digital Watermarking and Cryptography

A. *In short understanding:-*
IMAGE ⟵ Apply Digital Watermarking.
Digital Watermarked IMAGE ⟵ Apply Cryptography Techniques.

B.*Now Algorithm for Digital Watermarking & Cryptography:-*
Step 1: Read any JPG image.
Step 2: Source for Watermarking', 'SelectOption',
'2-D Signal','3-D Signal','4-D Signal','4-D Signal'
Step 2a: After this we have option for Base work and Improved work.
Step 2b: In Base work no Complexity addition to make more secure but in Improved Work Complexity also add for more security as Digital Signature and Embedding watermark.
Step 2c: Select textual image information and Embed with Original Image.
Step 3: [row,col,dim]=size(Data);
if (dim>1)
Step 4: Input image convert into grayscale image.
Step 5: Scaling and converting to binary
Step 6: Scaling to convert image into array of 8-pixels; each pixel is of 8 bits, therefore 8 pixel will be equals to 64 bit of data.
Step 7: Key Selection and Expansion, Input the key in the form of 133457799bbcdff1,
Example: - hex_key = '133457799bbcdff1';
[bin_key] = Hex2Bin(hex_key);
Step 8: Now Encryption and Decryption of image start
Step 9: orignal_msg=[];
encrypt_msg=[];
decrypt_msg=[];
for i=1:size(Data_binary,1)
Step 10: Generated Key applied to image Cipher
[cipher]=SF_Encrypt(orignal,K1,K2,K3,K4,K5);
encryption_time(i)=toc;
[plaintext]=SF_Decryption(cipher,K1,K2,K3,K4,K5);
encrypt_msg(:,i)=Binary2Dec(cipher);
decrypt_msg(:,i)=Binary2Dec(plaintext);

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 7, July 2015

Step 11: Converting the Vectors into Images
Original=uint8(reshape(Data,[row,col]));
Encrypted=uint8(reshape(encrypt_msg,[row,col]));
Decrypted=uint8(reshape(decrypt_msg,[row,col]));
Step 12: Plot the graph of figure.
Step 13: Calculating the Encrypted and Original image's Entropy.

IV. SIMULATION AND RESULTS

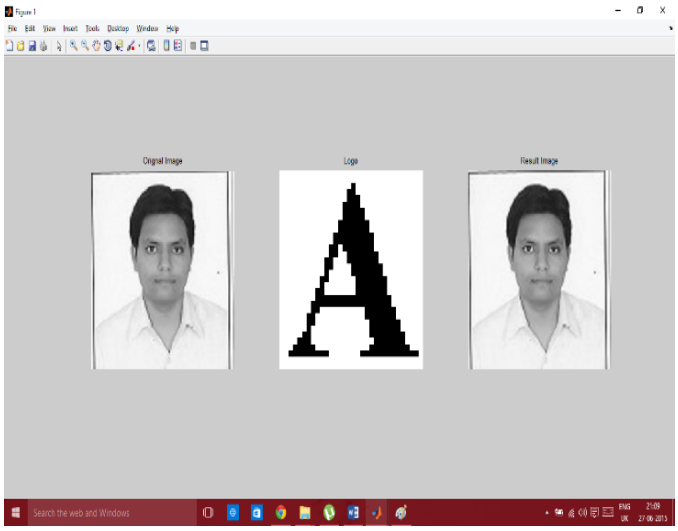

Fig 1: Digital watermarking applied to Original image with text information

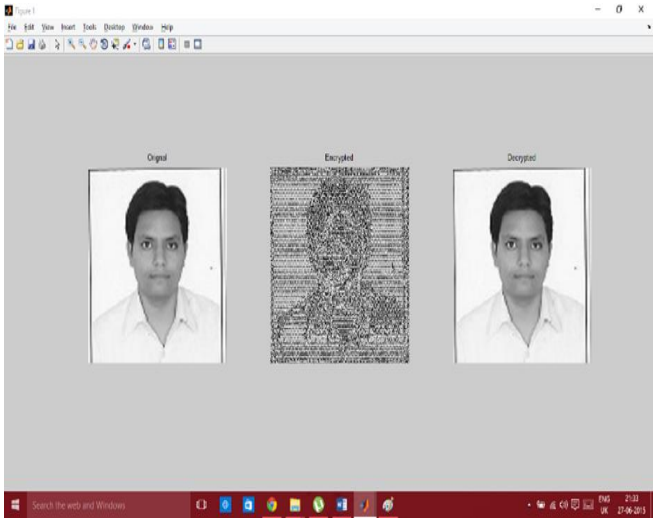

Fig 2: Encrypted & Decrypted Image with information.

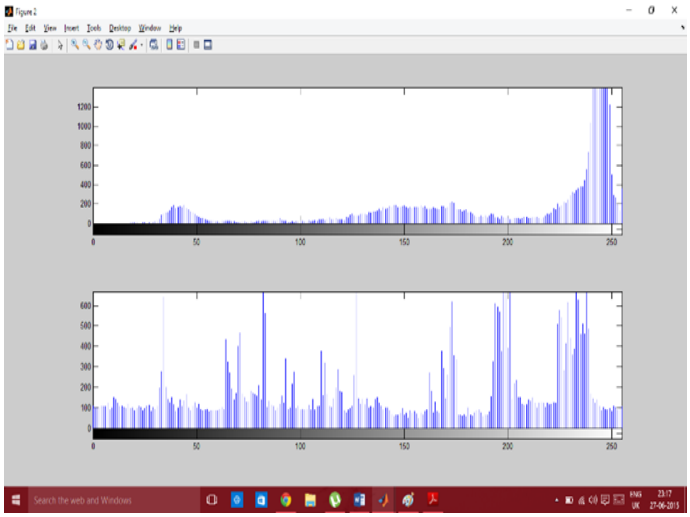

Fig 3: Histogram showing Original and Encrypted image.

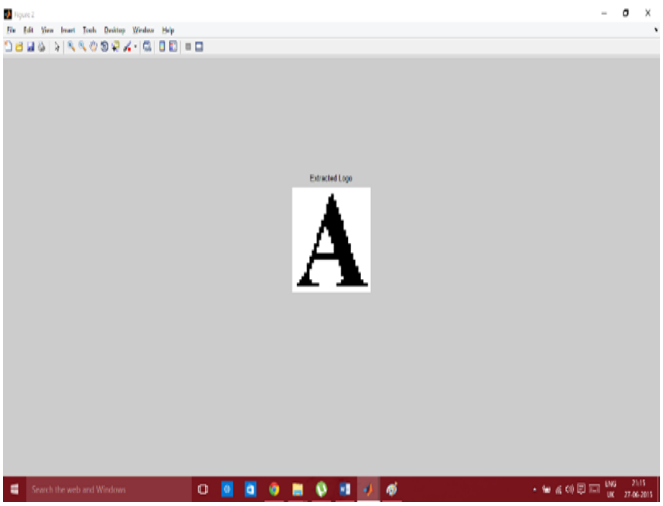

Fig 4: Extracted Textual information image.

C. *Information about Extracted Original image*
PSNR = Inf
BER =1.855469e-02
NC =7.480469e-01
D. *Information about Encryption to Decryption time Elapsed*

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 7, July 2015

DoneElapsed time is 1.121985 seconds.
Re = 6.2399 7.5272

V. NOW ONLY TEXTUAL DATA TYPED INFORMATION HIDING WITH WATERMARKING AND WITH DES SYMMETRIC CRYPTOGRAPHY WITH SIMULATION

Step 1: select the image flower.jpg (any jpg can select) by clicking on Load image in fig 5.

Fig 5: select image for text watermark

Step 2: Write any text (here I write name JAI SINGH) **to** embed.

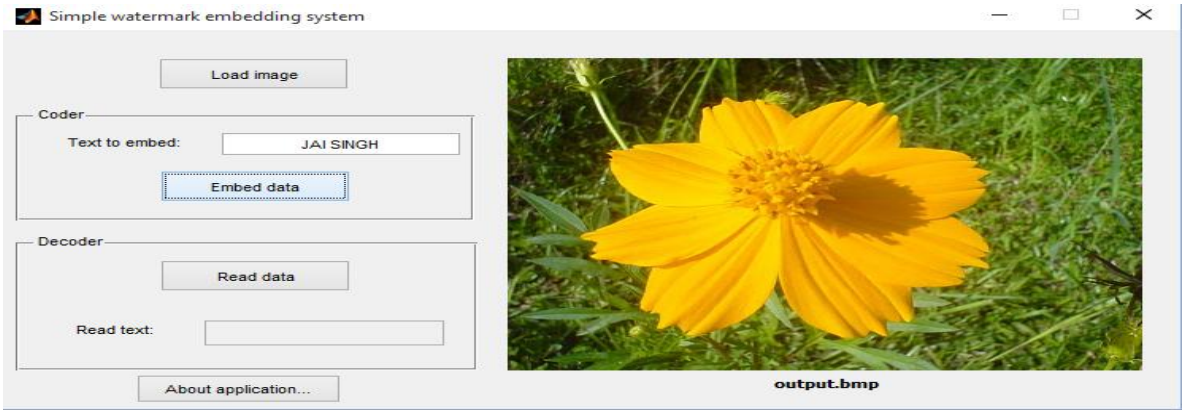

Fig 6: Text to Embed into image

Step 3: when click on Embed data flower.jpg change into output.bmp in fig 6.
Step 4: Click on Read data it shows embed data in Read text in fig 6.
Now we Encrypt and Decrypt output.bmp with DES Symmetric Cryptography.Algorithm for DES Encryption and Decryption
In which we use Hundungen Key and formed matrix bitxor
a1(i,j,1)=bitxor (a1(i,j,3),a1(i,j,1));
a1(i,j,2)=bitxor (a1(i,j,1),a1(i,j,2));

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 7, July 2015

a1(i,j,3)=bitxor (a1(i,j,2),a1(i,j,3));

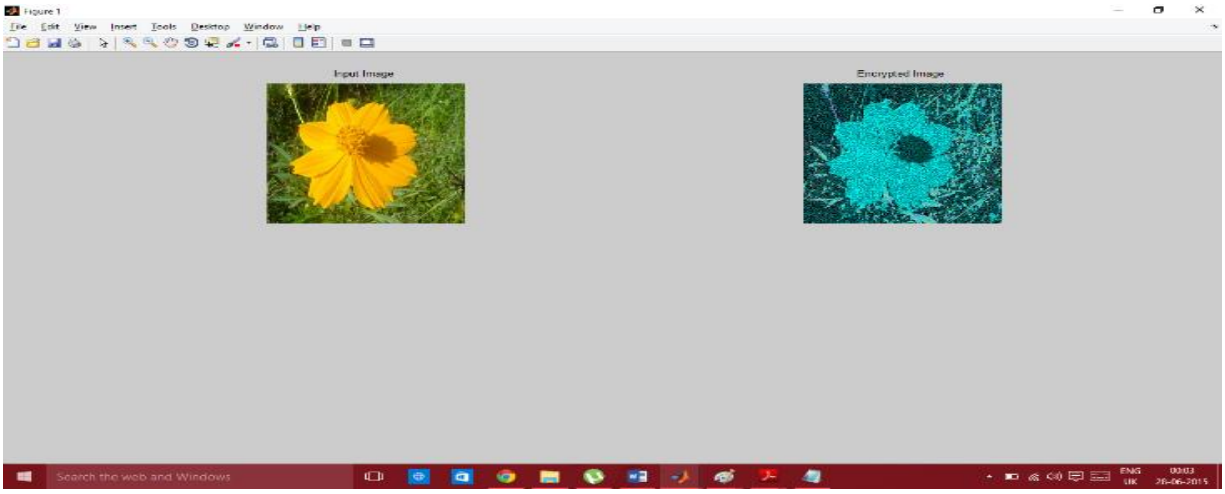

Fig 7: Input output.bmp image for encryption

Step 5: Now apply DES encryption any numeral Key (0-1), (I use numeral 2 key for Encryption in fig 7.
Step 6: For Decryption again Enter same key as we use for Encryption so we enter 2 key again.
Step 7: Now successfully image Decrypted and histogram of Encrypted and Decrypted image plotted, see fig 8 and 9.

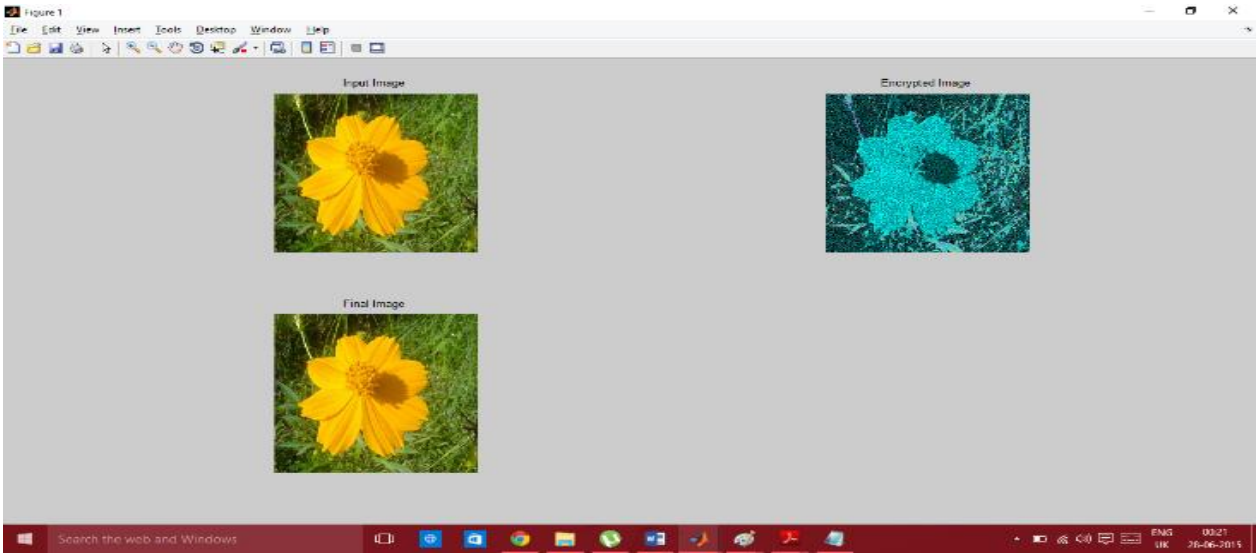

Fig 8: Final Decrypted image

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 7, July 2015

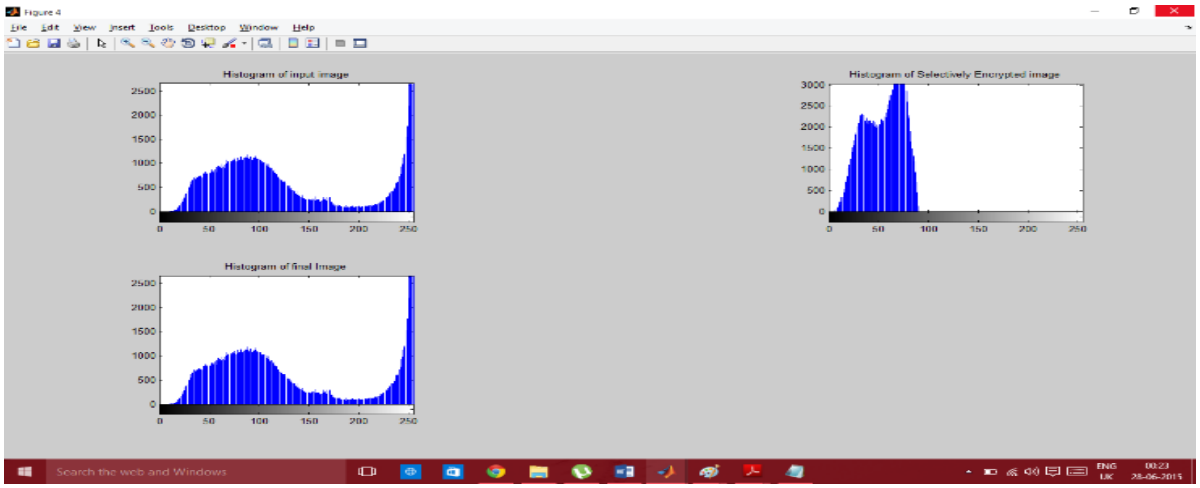

Fig 9: Histogram of input image and output image

Elapsed time is 0.618265 seconds in DES encryption.
Step 8: Now we take output.bmp image for text encryption fig 10, here we load output.bmp image file it contain text JAI SINGH which is decode when click on Read data.

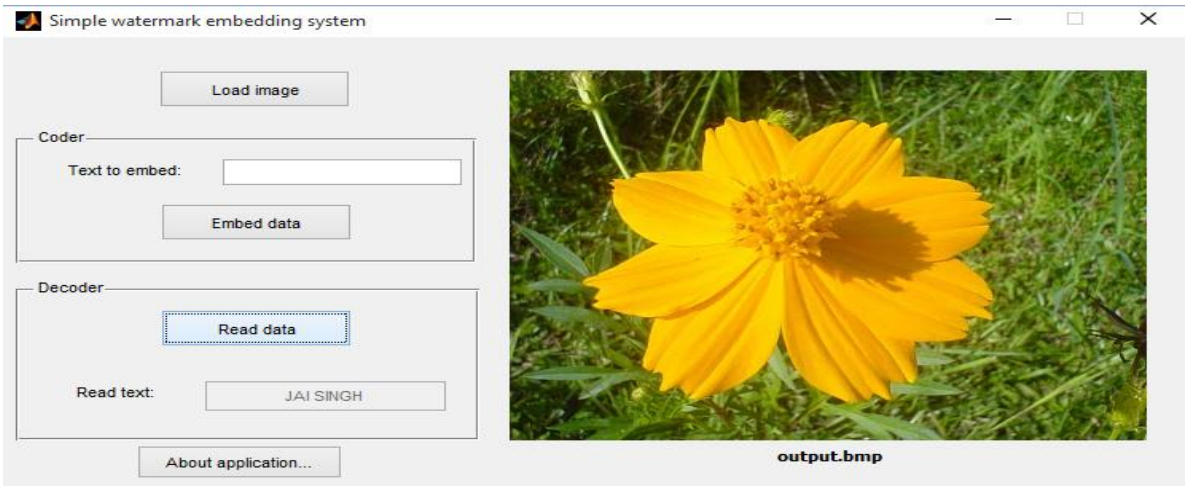

Fig 10: Decoded the Embed data to Read text

VI. CONCLUSION AND FUTURE WORK

From e-mail to cellular communications, from secure Web access to digital cash, cryptography is an essential part of today's information systems. Cryptography helps provide accountability, fairness, accuracy, and confidentiality. In the future, as commerce and communications continue to move to computer networks, cryptography will become more and more vital.But the cryptography now on the market doesn't provide the level of security it advertises. Most systems are not designed and implemented by cryptographers, but by engineers who think cryptography is like any other computer technology. It's not. You can't make systems secure by tacking on cryptography as an afterthought. You have to know what you are doing every step of the way, from conception through installation.

We need to improve our understanding of, and methodologies for, designing cryptographic standards. For widely used higher-level cryptographic protocols (e.g., TLS, WiMax, IPsec), we end up using standards that are designed by public

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 7, July 2015

committees such as those formed by the IETF. While we do not want to denigrate the hard work and expertise of those involved, it's clear that there are limitations to this approach and the results can sometimes be disappointing.
We advocate research and experimentation on new design approaches for cryptographic standards. Most of the modern Cryptographic has focused on security definitions and proofs that construction achieve them. This is a powerful approach but does not always account for robustness when security definitions are narrow. So we need develop Hybrid encryption concept which enhance higher security for any data over network.

VII. ACKNOWLEDGMENT

I would like to thank especially Assit. Prof. Kamil Hasan and Assit. Prof. Ravinder Kumar for valuable help in this topic Cryptographic and Hybrid combination encryption concept, Assit. Prof. Ravinder Kumar for assisting with data collection and stimulus preparation of the Hybrid Cryptographic Technique with Digital watermarking studies and it's coding, and also thankful of my friend Kanak Lata, Mohd. Firoz Alam and Veena Maurya for helping with collection of all data and ideas for Encryption. This works truly done under M.tech Research group in AL-Falah University.

REFERENCES

1. Jai Singh; Kanak Lata; Javed Ashraf, (2015). Image Encryption & Decryption with Symmetric Key Cryptography using MATLAB, International Journal of Current Engineering and Technology E-ISSN 2277 – 4106, P-ISSN 2347 – 5161 ©2015 INPRESSCO®, All Rights Reserved, Available online 25 Feb 2015, Vol.5, No.1 (Feb 2015)
2. Jai Singh; Mohd Firoz Alam; Assit. Prof. Kamil Hasan, (2015), Encryption and Decryption of Textual Data with Symmetric Key Cryptography and Improved Des Method Based on Irrational Number, International Journal of Research (IJR) e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 4, April 2015.
3. Kumar, M.; Hensman, (June 2013) A., Robust digital video watermarking using reversible data hiding and visual cryptography, Signals and Systems Conference (ISSC 2013), 24th IET Irish , vol., no., pp.1,6, 20-21 doi: 10.1049/ic.2013.0051
4. Fouad, M.; El Saddik, A.; Jiying Zhao; Petriu, E., (2011) Combining cryptography and watermarking to secure revocable iris templates, Instrumentation and Measurement Technology Conference (I2MTC), IEEE , vol., no., pp.1,4, 10-12 May 2011doi: 10.1109/IMTC.2011.5944015
5. Bhargava, N.; Sharma, M.M.; Garhwal, A.S.; Mathuria, M., (2012), Digital image authentication system based on digital watermarking, Radar, Communication and Computing ICRCC, 2012 International Conference on, vol., no., pp.185,189, doi:10.1109/ICRCC.2012.6450573
6. Shing-Chi Cheung, Dickson K. W. Chiu, and Cedric Ho. (2008). The use of digital watermarking for intelligence multimedia document distribution. J. Theor. Appl. Electron. Commer. Res. 3, 3 (December 2008), 103-118.
7. Stelvio Cimato, James Ching-Nung Yang, and Chih-Cheng Wu. (2012). Visual cryptography based watermarking: definition and meaning. In Proceedings of the 11th International conference on Digital Forensics and Watermaking (IWDW'12), Yun Q. Shi, Hyoung-Joong Kim, and Fernando Pérez-González (Eds.). Springer-Verlag, Berlin, Heidelberg, 435-448. DOI=10.1007/978-3-642-40099-5_36 http://dx.doi.org/10.1007/978-3-642-40099-5_36
8. I-Kuan Kong and Chi-Man Pun. (2008). Digital Image Watermarking with Blind Detection for Copyright Verification. In Proceedings of the 2008 Congress on Image and Signal Processing, Vol. 1 - Volume 01 (CISP '08), Vol. 1. IEEE Computer Society, Washington, DC, USA, 504-508. DOI=10.1109/CISP.2008.546 http://dx.doi.org/ 10.1109/CISP.2008.546
9. Huiping Guo. (2003). Digital Image Watermarking for Ownership Verification. Ph.D. Dissertation. University of Ottawa, Ottawa, Ont., Canada, Canada. Advisor(s) Nicolas Georganas. AAINQ85364.
10. Singh, T.R.; Singh, K.M.; Roy, S., (2012) Robust video watermarking scheme based on visual cryptography, Information and Communication Technologies (WICT), World Congress on, vol., no., pp.872,877, Oct. 30 2012-Nov. 2 2012 doi: 10.1109/WICT.2012.6409198
11. Cox, J.; Miller, M. L.; Bloom, J. A.; Fridrich J. & Kalker T. (2008). Digital Watermarking and Steganography, Morgan Kaufmann Pub., Elsevier Inc.

BIOGRAPHY

Jai Singh is a M.tech Scholar in the Electronics and Communication Engineering Department, Al-Falah University, Received B.tech Degree from Maharshi Dayanand University in 2012, Pursuing M.Tech from Al-Falah University. Mainly Research in the field of Computer Networks and Wireless Communications.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 7, July 2015

Kamil Hasan is a Research Assitant in the Electronics and Communication Engineering Department, Al-Falah University, Received M.tech Degree from Maharshi Dayanand University, Mainly Research in the field of Digital Signal Processing, VLSI, Computer Networks and Wireless Communications.

Ravinder Kumar is a Research Assitant in the Electronics and Communication Engineering Department, Al-Falah University, Received M.tech Degree from Maharshi Dayanand University, Pursuing PH.D from Maharshi Dayanand University Mainly Research in the field of Optical Fiber channel, VLSI, Computer Networks and Wireless Communications.