An Efficient and Secure Multi-Layered Image Steganography Approach Using LSB and Lightweight XOR Encryption for Improving Time and Space Complexity

Research paper Author and project Group leader: - Soumik Sur, Project Mentor: - Raja Dey Assistant professor JIS College of Engineering
co-author:-Shubhankar Das, Sakshi Bose, and Sudip Dhauria All students are of B.Tech from JIS College of Engineering.

Abstract:-

Steganography is the practice of hiding information within another data in such a way that the presence of the hidden message is undetectable to causal observers. Encryption which makes data unreadable without a decrypt key, Steganography conceals the very existence of the data.

In steganography, data is embedded within a carrier medium such as Image, Audio files, video files, Text files, Network protocols.

But most popular among them is Image. For hiding secret information there exist a large variety of stenographic technique some are more complex than others and all of them have respective strong and weak points. Steganalysis, the detection of this hidden information, is an inherently difficult problem and requires a thorough investigation. So we are using LSB algorithm.

Beside Complex encoding in steganography we are also focus on time and space complexity because if we only make complex encoding in steganography then file size will increase and it will be a problem for file transfer and downloading.

This research presents a cutting-edge image steganography method that effectively and securely conceals data by combining Least Significant Bit (LSB) embedding with XOR-based lightweight encryption for maintaining Time and space complexity. The technique increases resistance to unwanted extraction by randomly distributing encrypted messages throughout the image using password-driven pixel randomization. A unique psychological component is included: users are presented with the statement, "Hidden Message will not get revealed," during their first attempt at decoding, which intentionally builds suspense and discourages inadvertent intrusions. The hidden content, which may be displayed in mirrored format to further obfuscate it, is revealed through subsequent interactions. Simple encoding and decoding procedures are made possible by the intuitive interface, which was created with Google Colab's ipywidgets. The method's feasibility for safe image-based information concealment is confirmed by experimental evaluations that show good fidelity with little distortion.

Keyword:-

Encoding, Decoding, cryptography, Steganography, Steganalysis, digital image, RGB image, Binary image, LSB, Psychological layer of Encoding, physics, optics physics,Reasoning,Verbal and Non-Verbal Reasoning, Embedded Figures, Mirror and Water Image etc.

Introduction:-

In the present world of internet data transfer grow rapidly so security is very important. So hiding the data within another data by metadata in the process of steganography is very much important in nowadays. It can be used for various purposes, including hiding sensitive data, secret communication, and digital watermarking. Steganography is different from Cryptography, which is the practice of encrypting information to keep it secret. Steganography can be used in digital media such as images, audio files, and Video files. But most popular among them is image steganography.

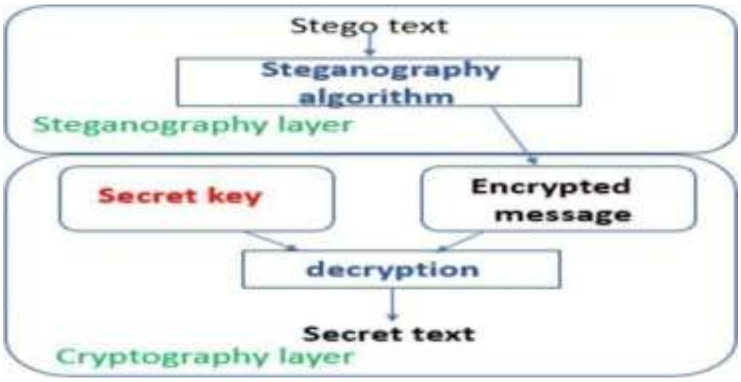


Fig. no 1

The term originates from the Greek Words "Steganos" (covered) and "graphia" (writing), meaning "covered writing". Though the term steganography originate from Greek but we can get the concept of algorithm of steganography from the India also which has a long history of encoding hidden messages and multi-layered meanings in art, it has a fundamental role in the conceptual origin of algorithms influenced by steganography. Mughal miniatures, temple murals, and the cave paintings of Ajanta and Ellora were examples of ancient art that was more than merely ornamental; they communicated philosophical, cultural, and spiritual concepts that were frequently reserved for the initiated. The current steganography technique of concealing information in plain sight is closely reflected in this symbolic layering. Indian art employed complex design, color symbolism, and visual metaphors to encode knowledge in order to both transmit and safeguard it. India is at the forefront of creative traditions that match computational steganography because of this intentional visual encryption, which makes Indian painting both historically relevant and philosophically aligned with data-hiding techniques.

Though their goals were frequently different, other civilizations also created art that was rich in symbolism. Over 40,000 years old, Australian Aboriginal rock art was used for rituals rather than covert communication. Although they lacked intricate narrative layering, the cave paintings at Altamira in Spain and Lascaux in France demonstrated early symbolic expressiveness. While Indonesian traditions in Java and Bali used symbolism in puppetry and temple carvings, frequently for ritual more than secret, Greek art explicitly depicted myth and philosophy. Mesoamerican codices, Egyptian paintings, Japanese ukiyo-e, and Chinese scrolls all expressed culture, but mostly in an explicit manner. More as artistic mystery, Renaissance Europe added secret features to da Vinci's Mona Lisa and The Last Supper. On the other hand, India is particularly significant because to its long-standing usage of encoded symbolism, which closely resembles contemporary stenographic objectives.

Psychological Layer of Encoding:-

The encoding procedure in this project is intended to build tension by first revealing the secret message when the "Decode" button is clicked. This notification appears instead of the message being revealed right away: "Hidden Message will not get revealed." Users become more involved in the decoding process as a result of this intentional delay, which appeals to the brain's innate curiosity and need for closure. The technique creates suspense and increases the final joy of discovering the hidden material by requiring user input to expose the message. This method uses psychological concepts to improve user engagement and memory retention in addition to making the experience more interactive.

Physics:-

The study of matter, energy, and the fundamental forces of nature is the focus of the scientific discipline of physics. From the tiniest particles to the biggest cosmic structures, it aims to comprehend how the universe functions. Physics describes natural occurrences and lays the groundwork for technological and scientific growth by examining ideas like motion, forces, energy, and their interactions. Relativity, quantum mechanics, thermodynamics, electromagnetic, and mechanics are important fields that collectively help us comprehend everything from the size of the universe to atomic behaviour. In the end, physics stimulates creativity in a variety of domains, including engineering and medicine, and aids in the explanation of the principles governing our physical universe.

Optics Physics:-

The study of light and how it interacts with matter is the focus of the physics field of optics. It focuses on comprehending how light behaves, particularly how it **reflects**, **refracts**, **diffracts**, and **disperses**. The study of optics describes how light moves, is affected by mirrors and lenses, and interacts with various substances. Physical optics, which investigates the wave- like properties of light, such as interference and polarization, and geometrical optics, which studies light routes and image formation, are both included in this discipline. In many scientific, medical, and engineering applications as well as in technologies like telescopes, lasers, fibre optics, and microscopes, optics is essential.

How Optics Physics is used in this project:-

The basic ideas of light and picture production make optics physics indirectly relevant to this research. Using optical lenses and sensors, which have their roots in optics, digital images used in steganography are produced by collecting light reflected from objects. To conceal data, the project manipulates pixel values, which stand for color and light intensity. Visual decoding, which includes the mirror-text effect, simulates optical reflection in the real world. Furthermore, the stego image depends on the light coming from screens and the way the human eye interprets it, both of which are aspects of optics. Therefore, optics supports the project's core picture capture, display, and perception even though it is not a part of the code.

Reasoning:-

The process of thinking rationally and coming to conclusions from facts, evidence, or provided information is known as **reasoning**. It entails context analysis, pattern recognition, issue resolution, and decision-making through meaningful concept connections. One can use **deductive** reasoning, which proceeds from general principles to particular conclusions, or **inductive** reasoning, which draws general conclusions from particular observations. It is a basic ability that is applied to academics, professional problem-solving, and daily living. Reasoning enables people to assess arguments, comprehend relationships, and make wise decisions. It is crucial for courses like physics, math, philosophy, and competitive tests where logical analysis and critical thinking are crucial.

Nonverbal Reasoning:-

Non-verbal reasoning is a kind of logical thinking in which **visual information** is used instead of words or figures to analyse and solve problems. It assesses your comprehension and interpretation of sequences, diagrams, patterns, and shapes. ****Series completion**, **mirror images**, **pattern recognition**, **figure classification**, **and paper folding**** are examples of common nonverbal reasoning questions. This type of reasoning is helpful for evaluating intelligence across linguistic backgrounds because it assesses **spatial awareness, logical thinking, and problem-solving skills** without depending on language. In order to examine a person's **visual and abstract thinking abilities**, nonverbal reasoning is frequently incorporated into competitive exams, IQ tests, and admission exams for schools and jobs.

How Mirror and Water Image concept of physics come under Nonverbal Reasoning?

In nonverbal reasoning, **mirror and water images** are visual tasks that assess a person's capacity to mentally flip or reverse characters, numbers, or forms. Despite being grounded in the principles of light reflection in physics, they are utilized in reasoning to evaluate **spatial imagery and logical thinking** rather than scientific comprehension. Whereas a **water image** reflects horizontally (top-bottom reversal), a **mirror image** reflects vertically (left-right reversal). These kinds of questions assess a person's ability to cognitively manipulate items and comprehend patterns, which is helpful in aptitude tests and exams.

Because they only use **visual analysis** and do not rely on language or numerical data, they are an important component of non-verbal thinking.

What are the Verbal and non-verbal reasoning used in this project?

****Verbal reasoning**** in this project refers to the analysis and interpretation of information conveyed through words, including the comprehension of logical sequences, analogies, and language-based patterns. Conversely, **non-verbal reasoning** emphasizes spatial and visual comprehension without the need of language. Important elements of nonverbal thinking include **embedded figures**, which assess pattern recognition and attention to detail by having participants identify a basic shape concealed within a complicated design.

Mirror images emphasize lateral inversion and evaluate the ability to visualize how items appear when reflected across a vertical axis. The ability to visualize vertically inverted things as though they were reflected on a water surface is required for **water images**, which tests one's spatial orientation abilities. Together, these components improve language and visual-spatial reasoning skills, which in turn improve cognitive ability.

Literature Survey :-

The research of several video stegano techniques is additions of image-based stegano techniques. The research founds the various works from different authors.

- **K.Gopala Krishna & A. Bhattacharyya (2012):** The authors proposed a modified LSB technique that dynamically adjusts the embedding process based on the statistical properties of the image. This approach reduces distortions and makes the steganographic process harder to detect through steganalysis.

- **T.Morkel et al. (2013):** Focused on comparing different LSB techniques, such as fixed location and random-pixel LSB methods. The study highlighted the superiority of random-pixel LSB in avoiding detection by statistical analysis methods.

- **R.Munshi & S.Patil (2015):** Introduced a technique combining LSB with edge-detection algorithms. The method embeds secret data only in the edge regions of the image, preserving image quality and enhancing security by targeting high-complexity areas.

- **N.Selvi & P. K. Meena (2016):** Developed a multi-layered steganographic approach, where LSB is applied iteratively on multiple layers of an image, significantly increasing the embedding capacity while maintaining a visually unchanged carrier image.

- **A.Banik & A.Acharya (2018):** Proposed an optimized LSB technique for video steganography. Their method hides data in selected frames of a video sequence using pixel intensity changes, offering a balance between security and computational efficiency.

- **J. Singh & M.Kaur (2019):** Enhanced LSB by integrating cryptographic techniques such as AES encryption prior to embedding. This hybrid model ensures the data remains secure even if extracted by unauthorized users.

- **H.Khan&R.Roy (2020):** Explored the impact of image compression formats (JPEG vs. PNG) on LSB steganography. Their research demonstrated that lossless formats (e.g., PNG) are more suitable for LSB techniques due to the preservation of embedded data.
- **M.Hossain et al. (2021):** Designed a reversible LSB data-hiding algorithm that allows both the secret data and the original image to be completely restored after extraction. This is especially relevant in medical or forensic image processing.

- **A.Sharma & K.Jain (2022):** Presented a chaos-based stenographic model that uses pseudo-random number generators for embedding, making the method resilient against steganalysis while increasing data embedding capacity.

- **P. Chatterjee & A. Das (2023):** Studied deep learning-based adaptive LSB embedding. The model learns optimal embedding patterns by analyzing the carrier image’s structure, significantly improving robustness against AI-powered steganalysis.

- **S. Thakur &N. Jain (2023):** Discussed multi-carrier steganography by embedding data into multiple image formats (e.g., PNG, BMP, TIFF) simultaneously using LSB. This technique distributes the risk of detection and ensures higher security.

- **A.Roy & R.Saha(2024):** Focused on real-time applications of LSB steganography in IoT devices, embedding sensitive data within transmitted sensor data streams. Their method improves the security of real-time communication

Proposed System

The Least Significant Bit (LSB) technique is used in the suggested system, a secure picture steganography application that enables users to insert and extract hidden messages within PNG images. By using password-driven pixel shuffling and XOR-based encryption, it improves on basic LSB steganography and guarantees anonymity and detection resistance.

Key Feature:

1. **LSB-Based Message embedding**

The least important portions of an image's pixels are used to contain secret messages after they have been translated to binary.

To preserve image quality, just the red channel of pixels is utilized.

2. **XOR encryption:**

A basic XOR key is created using the password that the user has supplied.
To add an additional degree of protection, the message is encrypted using XOR prior to embedding.

3. **Pixel shuffling based on a password:-**

The pseudo-random generator is seeded with the password.

Without the right password, extraction becomes challenging because this dictates the sequence in which pixel coordinates are used for embedding.

4. **Interface (UI) that is easy to use:-**

Ipywidgets were used in its construction to make Google Colab easier to utilise.

Users can download the stego-picture after uploading a PNG image and entering their password and secret message.

5. **Three-Step Message Disclosure:-**

To improve security and engagement, the suggested system employs a novel three- step message disclosure technique. The method creates suspense and curiosity for the user by introducing a psychological encoding layer in the **first step**. This layer emits a message stating that the secret message will not be exposed. The **second step** adds a layer of visual encryption based on reflection principles and renders the concealed content illegible at a glance by displaying it in a visually modified **mirror text format**. The **third step** completes the sequential revelation and strengthens user involvement and security by fully disclosing the secret content in its original readable form.

Security Benefits:-

- Randomized embedding makes it more difficult for attackers to find or retrieve buried data.
- Without the right password or key, the message cannot be recovered.
- The look of the image is preserved since embedding only modifies one bit per pixel.

Goals:-

- The objective is to create a steganography tool that is both lightweight and efficient.
- To use LSB for message hiding and simple encryption.
- To improve security by randomly placing data using a password.

Time and Space Complexity Table – Advanced Image Steganography

Component	Operation	Time Complexity	Space Complexity	Explanation
xor_encrypt_decrypt	XOR each character of the message with a key	O(n)	O(n)	n = length of the message
message_to_binary	Convert message to binary + add 32-bit length prefix	O(n)	O(n)	8 bits per character plus a 32-bit prefix
binary_to_message	Convert binary string back to message	O(n)	O(n)	Each 8 bits are converted to a character
get_shuffled_positions	Generate and shuffle pixel positions	O(w × h)	O(w × h)	w = width, h = height; all pixels are shuffled
encode_image	Modify LSB of red channel for each bit	O(b)	O(1) + O(b)	b = number of bits in binary message
decode_image	Read LSBs and reconstruct message	O(b)	O(b)	b = 32 + length of embedded message
mirror_text	Reverse and replace with mirrored characters	O(n)	O(n)	One pass for reversing and one for mapping
UI (Widgets)	Display, input, file upload	O(1)	Depends on usage	Basic interaction, bounded by frontend environment

Why this steganography project's Time and Space Complexity is better and Unique than other's?

Because this project effectively balances lightweight encryption, randomized embedding, and format flexibility, its time and space complexity is superior to and more distinctive than that of conventional steganography techniques. It employs a lightweight XOR-based encryption in place of complex algorithms like AES, which is quicker and uses less memory (O(n)), making it perfect for contexts with limited resources. By employing password-based pixel shuffling (O(w × h)), the system improves security by making embedding places random in contrast to simple sequential techniques (O(n)). Additionally, a 32-bit message length prefix is embedded, allowing for self-contained decoding without the need for extra metadata. An additional layer of obfuscation is added at little cost by the multi-step reveal with mirror-text. Additionally, it is efficient and widely compatible, supporting.png,.jpg, and.jpeg formats without the need for extra processing.

Methodology:-

The process uses XOR-based lightweight encryption in conjunction with LSB steganography to encode a secret message into an image. Prior to being embedded into the least significant bits of shuffled pixel positions created using the same password as a seed, the message is first encrypted using a password-derived key and then transformed to binary with a 32-bit length prefix. The positioning of the data is unpredictable thanks to this randomized embedding, which increases security. In order to extract and decrypt the message, the same password is used to regenerate the pixel order. The message is gradually displayed through a three-step reveal procedure that includes a psychological layer and a mirrored text stage for more human-centric obfuscation. Multiple image formats (.png,.jpg, and.jpeg) are supported by the system, providing flexibility and low computing overhead appropriate for secure and useful stenographic communication.

Method:-

To safely conceal and recover messages in PNG images, the project combines XOR encryption, password-based randomization, and the Least Significant Bit (LSB) steganography approach.

The following steps make up the method**:-**

1. Preparing the input:-

An image in PNG format (cover image), A coded message,
A key or password.

Conversion of Messages.

The password is transformed into a numerical key and the secret message is encrypted using a straightforward XOR cypher.

A binary string is created from the encrypted message.

To aid with extraction, the binary message's length is saved as a 32-bit prefix.

2. Shuffling of Pixel Positions:-

All pixel coordinates are calculated using the image's width and height.

The password is used as a seed to create a pseudo-random shuffle of pixel locations.

This makes detection more difficult by guaranteeing that the data is concealed in random pixel places rather than in sequential sequence.

3. Embedding of LSB:-

The selected pixels' red channel's least significant bits (LSBs) contain the binary message. There is very little visual distortion because each pixel just has one bit changed.

4. Generation of Stego Images:-

A new PNG file with the altered image is saved.

This "stego-image" is available for download; it has the same visual appearance as the original but hides the message.

5. **Extracting Messages (Decoding):-**

After entering the password, the user uploads the stego-image. The password is used to replicate the same pixel shuffling.

The message length is calculated by extracting the first 32 bits.

The same XOR technique is used to decode the message bits after they have been read from the scrambled pixels.

At first decoding button click it show “The hidden message will not get revealed”this psychological layer is used to create Suspense, confusion to the hacker’s.

Then in second click of the decoding button Mirror image of the Original message is show so is unreadable to the hackers.

In the third click of the decoding button it shows the original hidden message.

Experiment and Results:-

The experimental setup, test cases, and results of utilizing the suggested LSB-based steganography system with password-driven pixel randomization and XOR encryption are shown in this section.

Experimental setup:-

- Google Colab (a Python environment)
- Pillow, ipywidgets, base64, and random libraries were used.
- PNG (lossless compression) is the image format.
- Test Images: Common pictures with different sizes (e.g., 256×256, 512×512)
- Plaintext strings of different lengths are used for secret messages.
- Tested passwords were alphanumeric ones with varying lengths.

Procedure:-

1. The user interface was used to upload a PNG picture.
2. They gave a password and a secret message.
3. The program implanted the message into LSBs of randomly chosen pixels after converting it to binary and encrypting it using XOR.
4. They created and downloaded a stego-image.
5. The message was extracted, decrypted, and the same password was used for decoding.

Experimental Results:-

Test No.	Image Size	Message Length (chars)	Password Used	Encoding Time	Decoding Time	Success	Notes
1	256×256	50	pass123	~0.3 sec	~0.2 sec	✅ Yes	Message recovered fully
2	512×512	150	Secretkey	~0.4 sec	~0.3 sec	✅ Yes	Works on larger images
3	128×128	300	Wrongpass	~0.2 sec	~0.2 sec	❌ No	Garbled output due to incorrect password

4	300×300	200	mypwd	~0.3 sec	~0.2 sec	✅ Yes	Pixel quality unchanged

Visual Quality Check:-

- Observation: The original and stego-images did not appear to vary from one another to the naked sight.
- In conclusion, undetectable changes are guaranteed by the LSB embedding (1 bit per pixel).

Key Findings:-

- 100% of decoding attempts with the right password were successful.
- Security: Message extraction fails or produces junk if the password is incorrect.
- Performance: Even for high-resolution photos, encoding and decoding are quick.
- Capacity: Approximately 8,192 characters (one bit per pixel) can be safely embedded in a 256x256 picture (65,536 pixels).

Step by step Screenshot of how the project is working

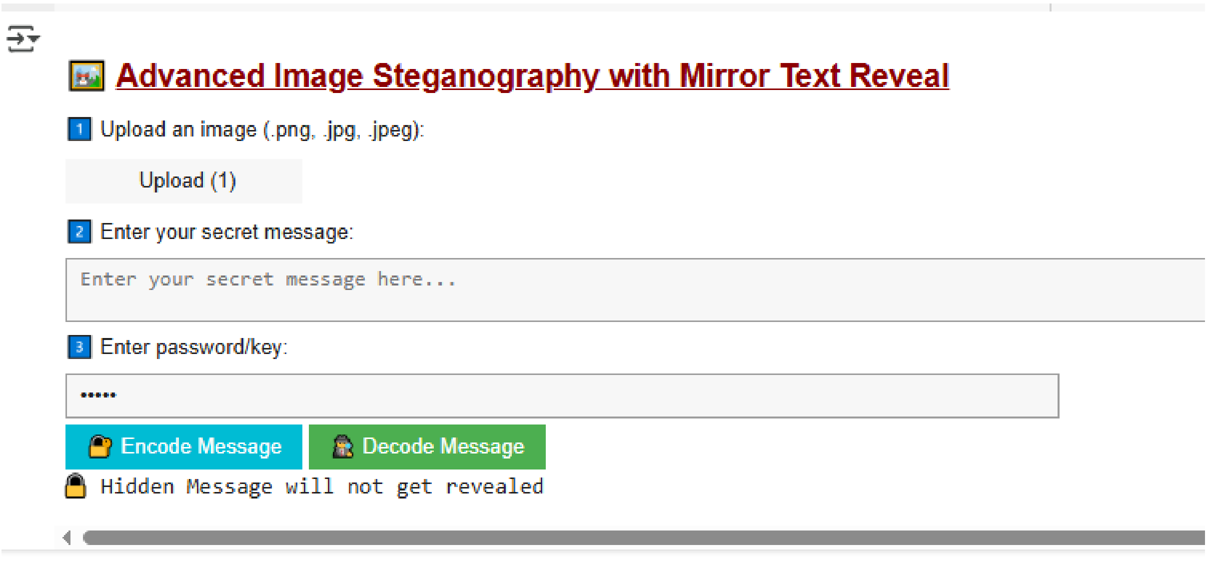
Step 1

Step 2
Image Given For Encryption

Step 3 Encoding

Step 4:

Stego image is produced with no change observed in naked eye



Step 5

Image produce after First click in decoding button it show "Hidden Message will not get revealed" to psychologically confuse the hacker

Step 5

Mirror image of the original message which is given is produced in second click in the Decoding button

Step 6

Finally at third Click the Original image is produced

<u>Conclusion:-</u>

To sum up, this research offers a safe, effective, and intuitive image steganography solution that improves confidentiality and attack resistance by combining password-driven pixel position shuffling with lightweight XOR-based encryption with LSB. It provides flexibility and self-contained decoding by supporting different image formats (.png. jpg, and.jpeg) and incorporating a message length prefix. A special layer called Psychological layer which show “hidden Message will not get revealed” and human-centric obfuscation is added by the novel multi-step reveal procedure using mirrored text. The method's capacity to incorporate large messages without causing obvious image deterioration while maintaining fast processing times is confirmed by experimental results. Overall, the system is well-suited for actual stenographic applications since it achieves a balance between security, performance, and usability.

<u>References:-</u>

1] N. F. Johnson, S. Jajodia, “Exploring Steganography: Seeing the Unseen”, Computer Journal, IEEE, February 1998.

[2] M. M. Amin, M. Salleh, S. Ibrahim, M.R.Katmin, M.Z.I. Shamsuddin, “Information Hiding using Steganography” Proceedings of 4th National Conference on Telecommunication Technology, Shah Alam, Malaysia, 2003.

[3] N. Provos and P. honeyman, “Hide and seek: an introduction to steganography” IEEE Computer

Society, 2003.

[4] *K. Curran, X.Li, R. Clarke, "An investigation in to the use of the least significant bit substitution technique in digital watermarking", Journal of Applied Science 2 (3), pp. 648-654,2005.*

[5] *R. J. Anderson, F. A. P. Petitcolas, "On the limits of steganography", Journal of Selected areas in communications, 16(4), pp. 474-481, 1998.*

[6] *G. J. Simmons, "The prisoners problem and the subliminal channel", Proc. of CRYPTO, 1983.*

[7] *R. Chandramouli, M.Kharrazi, N. Memon, "Image Steganography: Concepts and Practice", proc. Of IWDW 2003, LNCS 2939, pp. 35-49, 2004.*

[8] *R. Radhakrishnan, K. Shanmugasundaram, N. Memon, "Data Masking: A Secure-Covert Channel Paradigm", 2002.*

[9] *D. Neeta, K. Sehal, "Implementation of LSB Steganography and its Evaluation or Various Bits", 2004.*

[10] *C. Cachin, "An Information Theoretic model for steganography", 2004*

[11] *J. Fridrich and M. Goljan, "Digital image steganography using stochastic modulation", SPIE Symposium on Electronic Imaging, San Jose, CA, 2003.*

[12] *A.D. Ker, "Steganalysis of LSB Matching in Grayscale Images", IEEE signal processing letters, vol. 12, No 6, 2005.*

[13] *K. B. Raja, N. Shankar, K. R. Venugopal, L. M. Patnaik, "Steganalysis of LSB Embedded Images using Variable threshold color pair analysis", IEEE 2006.*

[14] *C. Ming, Z. Ru, N. Xinxin, Y. Yixian, "Analysis of Curent Steganography Tools: Classification & Features", Proc. of International Conference o Intelligent Information Hiding and Multimedia Signal Processing, 2006.*

[15] *M. Niimi, H. Noda, E. Kawaguchi, "High Capacity and Secure Digital Steganography to Palette Based Images", 2002.*

[16] *N. Wu, M. Hwang, "Data Hiding Current Status and key issues", International Journal of Network Security, Jan 2007.*

[17] *W. Luo, "Object-related illustration watermarks on cartoon images", Feb 2004.*

[18] *R. Alwan, F. Kadhim, A. Al-Taani, "Data Embedding based on better use of bits in image pixels" International Journal of signal processing, 2005.*

[19] *K. M. Singh, L. S. Singh, A. B. Singh, K. S. Devi "Hiding Secret Message in Edge of the Image" International conference of Information and Communication Technology, ICICT 2007.*

[20] *J. Silman, "Steganography and staganalysis: An overview", SANS Institute 2001.*

[21] *T. Jamil, "Steganography: The art of hiding information is plain sight", IEEE potentials, 1999.*

[22] *H. Wang, S. Wang, "Cyber warfare: steganography vs. staganalysis", communication of the ACM, Oct 2004.*

[23] *L.M. Marvel, Jr. C.G. Boncelet, C. Retter, "Spread spectrum steganography" IEEE Transactions on Image Processing, 1999.*

[24] *I.Avcibas,N.Memon,B. Sankur,"steanalysis using image quality metrics" IEEE Trasactions on Image Processing, Feb 2003.*

[25] *J.R. Kreen, "Steganography And Steganalysis", jan 2004.*