International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

CRYPTIC COMMUNICATION: CONCEALING DATA WITH DCT IMAGE STEGANOGRAPHY

Dr.S.Durga Devi [1], S.Abisankar [1], A.Allwin Samuel [3], V.Aravindhan [4].

[1]Associate Professor, Computer Science and Engineering, Vel Tech High Tech Dr. Rangarajan Dr. Shakunthala Engineering college, Avadi
[2]UG Student, Computer Science and Engineering, Vel Tech High Tech Dr. Rangarajan Dr. Shakunthala Engineering college, Avadi
[3]UG Student, Computer Science and Engineering, Vel Tech High Tech Dr. Rangarajan Dr. Shakunthala Engineering college, Avadi
[4]UG Student, Computer Science and Engineering, Vel Tech High Tech Dr. Rangarajan Dr. Shakunthala Engineering college, Avadi

ABSTRACT :

Our day-to-day life is very much impacted by the usage of various websites and applications which require our own user credentials which may contain the details of the user. This data is encrypted and stored, and decrypted when necessary. But due to the advancement of technology, this data can easily be breached by a third-party member or a hacker. To prevent these kind of data breaches and for the safety of user data. Image steganography in websites is a technique that enables the hiding of sensitive data within images to protect it from unauthorized access. By embedding data within the pixel values or metadata of images, this method provides a covert means of communication and enhances data security. This paper explores the concept of image steganography in websites, discussing its advantages, limitations, and considerations. The camouflage effect offered by hiding data within images makes it difficult for attackers to detect the presence of hidden information. This technique adds an extra layer of security, making it challenging for unauthorized users to access or intercept the hidden data. However, the capacity and image quality limitations, as well as the potential for detection, should be carefully considered when implementing image steganography in websites. Compatibility with different platforms, devices and image formats is also crucial factor to ensure seamless integration.

Keywords: Data Encryption, DCT, hash function, Image Steganography, Secure Communication, Steganalysis, Digital Watermarking, Information hiding.

INTRODUCTION:

In today's computerized age, information security has gotten to be a need. As touchy data is transmitted and put away over different stages and systems, assurance from unauthorized get to and interferences is fundamental. Picture steganography has demonstrated to be a promising innovation in the field of information security, giving undercover communication and information assurance. Utilizing picture steganography has a few preferences over conventional encryption methods. To begin with, it speaks to a incognito communication channel, as the covered up information cannot be promptly uncovered by visual review. This property is particularly valuable in circumstances where privacy is vital, such as incognito communications and clandestine operations. Moment, picture steganography includes an additional layer of security to your security. Indeed if an assailant has get to to the picture, the covered up data will stay covered up unless they have information of the steganography method utilized and can effectively extricate the implanted information. Furthermore, picture steganography may serve as a shape of camouflage. In a computerized world ruled by pictures, covering up the information contained in pictures permits for consistent integration over stages and makes it less likely that a potential aggressor will distinguish the nearness of touchy data. . Be that as it may, it is vital to be mindful of the confinements and challenges related with picture steganography. Components such as measure and picture quality confinements, potential for discovery by progressed explanatory methods, and compatibility issues between diverse stages and picture groups ought to be considered. Encryption is a information change that scrambles information into ciphertext, a good for nothing shape that no one can studied unless they have the key to unscramble it. Information obscurity innovation makes a difference cover up delicate information imperceptibly inside carriers. Carriers are advanced media such as content, sound, pictures, video, interactive media, and are called envelopes of delicate information. Information stowing away comprises of two primary regions: steganography and watermarking.

Hash work is a work that changes over numbers or images into a littler number that can be utilized. The coordinated numbers esteem is utilized as an file in the hash table. There are various hash capacities accessible, and unused ones are created intermittently to address security concerns and make strides execution. A few well-known hash capacities that have been broadly utilized in the past

Encryption is a information change that scrambles information into scrambled content and a insignificant shape which no one can studied unless they have the key to unscramble the encryption.

A discrete cosine transform (DCT) communicates a limited grouping of information focuses in terms of a whole of cosine capacities wavering at diverse frequencies.

Existing System:

In existing framework When a client sets a secret word, it is not put away straightforwardly in its plain content frame. Instep, it is changed into a hash esteem utilizing a one-way hashing calculation. Commonly utilized calculations for secret word hashing incorporate bcrypt, Argon2, and PBKDF2. To encourage upgrade the security of watchword hashing, an interesting arbitrary esteem called a salt is created for each client. The salt is at that point combined with the user's watchword some time recently hashing. Salting makes a difference anticipate to utilize of precomputed tables (rainbow tables) to reverse-engineer passwords, as each user's salt is distinctive. The coming about hash esteem, along with the salt (on the off chance that pertinent), is put away in the website's database. The unique watchword is not put away at all. If an aggressor picks up unauthorized get to the database, they would as it were seen the hash values, making it amazingly troublesome to recover the genuine passwords. When a client endeavors to log in, the entered watchword goes through the same hashing prepare utilizing the put away salt (on the off chance that pertinent) and hashing calculation. The coming about hash is at that point compared with the put away hash esteem for that client. If the hashes coordinate, the secret word is considered substantial.

Proposed system:

Our demonstrate employments DCT calculation in steganography to store scrambled watchword of the client in a cover picture and store it in the database. To begin with the user's data is scrambled utilizing a key and at that point the scrambled shape is covered up into a picture by utilizing prime grouping steganography and put away in the database. The same calculation is taken after to reobtain the covered up data when vital. This unused

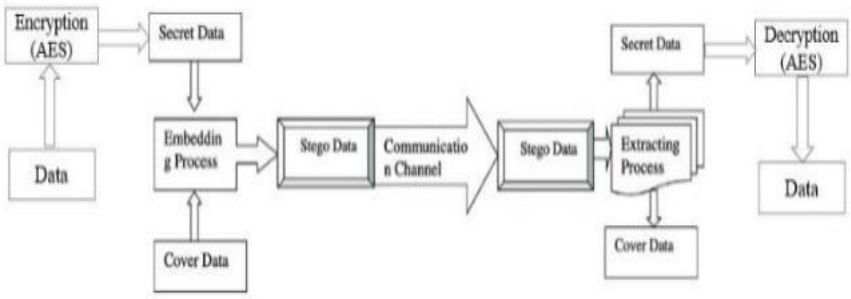

Fig.1 Block Diagram

Formula:

$$DCT(i,j) = \frac{1}{\sqrt{2N}}\, c(i)\, c(j) \sum_{x=0}^{N-1}\sum_{y=0}^{N-1} pixel(x,y) \cos\left[\frac{(2x+1)i\,\pi}{2N}\right]\cos\left[\frac{(2y+1)j\,\pi}{2N}\right]$$

$$C(x) = \frac{1}{\sqrt{2}}\ if\ x\ is\ 0, else\ 1\ if\ x > 0$$

method makes Beyond any doubt that the information is nearly incomprehensible to get breached too when the database is breached, as it were steganographic pictures are found and serve no reason to the Breacher.

Objectives

1. Steganography allows for the concealment of sensitive information within seemingly innocuous files or media
2. Steganography makes it difficult for adversaries to detect the presence of hidden information.
3. Storing passwords using steganography allows for distributing the password information across multiple files or media.
4. Low maintenance costs and easy to Implement.

Result:

Source Image

Output Image

steganography in websites is a fascinating technique that allows for the hiding of information within digital media, such as images, audio files, or even web pages themselves. It offers a means of covert communication or data concealment, making it an attractive option for various applications. Steganography in websites has both advantages and disadvantages. On the positive side, it provides a way to transmit sensitive or confidential information without raising suspicion or drawing attention. It can be particularly useful in scenarios where encryption or other conventional security measures might be insufficient or ineffective. However, steganography also presents challenges and potential risks. The hidden information may be vulnerable to detection or extraction by sophisticated algorithms or skilled adversaries. As a result, the level of security provided by steganography in websites depends on the complexity of the embedding algorithm and the strength of the concealment techniques used. Moreover, the use of steganography in websites raises ethical and legal concerns. While it can be employed for legitimate purposes, such as digital watermarking, copyright protection, or digital forensics, it can also be misused for illicit activities, including the covert exchange of sensitive information, spreading malware, or facilitating cybercrimes. As technology evolves, so do the methods of steganalysis (the detection of steganography). Researchers and security professionals continue to develop more sophisticated techniques to detect hidden information and improve the security of digital systems. Consequently, the cat-and-mouse game between steganographers and steganalysts is likely to persist. In summary, steganography in websites is a powerful and intriguing concept with a range of potential applications. It offers a way to hide information within digital media and can be used for legitimate purposes. However, it also comes with challenges, risks, and ethical considerations. As with any technology, its use should be guided by responsible and lawful practices to ensure its benefits are realized without compromising security or integrity.

Limitations:

It is important to note that image steganography has limitations and considerations.

(i) Capacity and image quality

a. The amount of data that can be embedded within an image is limited by factors like image size, factor and compression.

(ii) Robustness and detection

a. Sophisticated techniques and algorithms can be used to analyze images and detect the presence of hidden data.

(iii) Compatibility and standards

a. Compatibility across different platforms, devices and image formats should be considered.

Conclusion

In conclusion, steganography in websites is a fascinating technique that allows for the hiding of information within digital media, such as images, audio files, or even web pages themselves. It offers a means of covert communication or data concealment, making it an attractive option for various applications. Steganography in websites has both advantages and disadvantages. On the positive side, it provides a way to transmit sensitive or confidential information without raising suspicion or drawing attention. It can be particularly useful in scenarios where encryption or other conventional security measures might be insufficient or ineffective. However, steganography also presents challenges and potential risks. The hidden information may be vulnerable to detection or extraction by sophisticated algorithms or skilled adversaries. As a result, the level of security provided by steganography in websites depends on the complexity of the embedding algorithm and the strength of the concealment techniques used. Moreover, the use of steganography in websites raises ethical and legal concerns. While it can be employed for legitimate purposes, such as digital watermarking, copyright protection, or digital forensics, it can also be misused for illicit activities, including the covert exchange of sensitive information, spreading malware, or facilitating cybercrimes. As technology evolves, so do the methods of steganalysis (the detection of steganography). Researchers and security professionals continue to develop more sophisticated techniques to detect hidden information and improve the security of digital systems. Consequently, the cat-and-mouse game between steganographers and steganalysts is likely to persist. In summary, steganography in websites is a powerful and intriguing concept with a range of potential applications. It offers a way to hide information within digital media and can be used for legitimate purposes. However, it also comes with challenges, risks, and ethical considerations. As with any technology, its use should be guided by responsible and lawful practices to ensure its benefits are realized without compromising security or integrity.

REFERENCES :

1. Osama F. AbdelWahab, Aziza I. Hussein, Hesham F. A. Hamed, Hamdy M. Kelash, Ashraf A.M. Khalaf, Hanafy M. Ali"Hiding data in images using steganography techniques with compression algorithms" ResearchGate 2019.

2. Xiyao Liua , Ziping Maa , Zhihong Chena , Fangfang Li, Ming Jiang , Gerald Schaefer , Hui Fang: "Hiding multiple images into a single image via joint compressive autoencoders" Elsevier 2022.

3. Alejandro Martín, Alfonso Hernández, Moutaz Alazab, Jason Jung, David Camacho:"Evolving Generative Adversarial Networks to improve image steganography". Elsevier 2023.

4. Dalia Nashat, Loay Mamdouh: "An efficient steganographic technique for hiding data",2019.

5. Nandhini Subramanian, Somaya al-maadeed, Ahmed Bouridane: "Image Steganography: A Review of the Recent Advances", IEEE 2021.

6. Pengcheng Liu "Image encryption algorithm based on reversible information hiding and physical chaos in images" Elsevier 2023.

7. Jin Shang, Xiaobo Xu "Research on a double image security transmission algorithm of image encryption and hiding" Elsevier 2023.

8. Anggraeni Shinta Dewi; Hermawan Setiawan "Acceleration of Secure Hash Algorithm256 (SHA-256) on an FPGA-CPU Cluster Using OpenCL" International Symposium on Circuits and Systems(ISCAS) 2021.

9. Md. Simul Hasan Talukder; Md. Nahid Hasan; Rafi Ibn Sultan; Mahabubur Rahman; Ajay Krishno Sarkar; Sharmin Akter "An Enhanced Method for Encrypting Image and Text Data Simultaneously using AES Algorithm and LSBBased Steganography" International Conferemce on Advancement in Electrical and Electronic Engineering(ICAEEE) 2022.

10. Rutvik Dumre; Aashka Dave "Exploring LSB Steganography Possibilities in RGB Images" 12th International Conference on Computing Communication and Networking Technolgies(ICCCNT) 2021.

11. Sabah Abdulazeez Jebur, Abbas Khalifa Nawar, Lubna Emad Kadhim, Mothefer Majeed Jahefer "Hiding Information in Digital Images Using LSB Steganography Technique" ResearchGate 2023.

12. Nazmun Nhar; Md. Kawsher Ahmed; Tareq Miah; Shahriar Alam; Kh. Mustafizur Rahman; Md. Anayt Rabbi "Implementation of Android Based Text to Image Steganography Using 512-Bit Algorithm with LSB Technique" 5th International Conference on Electrical Information and Communication Technology (EICT) 2021.

13. Zhenyu Li, Hao Zhang, Xilin Liu, Chunpeng Wang, Xingyuan Wang "Blind and safety-enhanced dual watermarking algorithm with chaotic system encryption based on RHFM and DWT-DCT" Elsevier 2021.