Literature Review:

**Aparna, V. S., et al.in [1],** "Implementation of AES Algorithm on Text And Image using MATLAB", Proposed an encryption algorithm for the secure transmission of data. Advanced Encryption Standard (AES) a symmetric block cipher of 128-bits that uses the same key for encryption as well as for decryption is used. Here encryption and decryption are done on character message, string-text message, and image message. Plain text is inputted to encryption algorithm and output is an encrypted message i.e. ciphertext, then this ciphertext is given to decryption algorithm to get the decrypted message where plain text is reconstructed. This algorithm is highly efficient as decrypted output is the same as the input and there is no distortion in the output.

**Yashpal Lather et al. in [2],**” Review Paper on Steganography Techniques” discuss different steganography techniques their uses and limitation. Also, provide the difference between steganography and cryptography. Text, as well as different image steganography techniques, is mention in this paper. Lastly, it concluded that steganography that uses a key has better security than non-key steganography

**Arnold Gabriel Benedict et al. in [3]**, "Improved File Security System Using Multiple Image Steganography", proposed a slicing method where the secret data is sliced and stored on multiple cover images. The Least significant bit of all the selected cover image pixel values is used to hide the data this technique is called LSB based steganography technique. Payload which is a set of files that is to be hidden inside the cover file, are compressed using the ZIP compression algorithm. Image hashing algorithm ensures a random distribution of bits from compressed payload file; it has high latency in analyzing slicing pattern which makes it more difficult for the intruder to decrypt the pattern. Camouflage capacity or the capacity for hiding secret data in the cover image can be identified. Decoding follows equivalent steps as in encoding.

**Karolin., et al.in [4],** "Encryption and decryption of color images using visual cryptography" proposed a visual cryptography technique that allows digital images to be divided into multiple numbers of printable shares called transparent shares and transmitted physically by printing these shares on transparency sheets to the authorized users. Visual cryptography works on many forms of images such as grayscale images, black and white images as well as color images. Visual cryptography consists of three phases for color images. The first phase is to realize the color and print the color in the secret image on the shares directly. The second phase converts a color image into a black and white image; the third phases utilize the binary representation of the color of a pixel and encode the secret image at the bit-level. Computational complexity of traditional cryptography is overcome here. Blowfish algorithm is a 64-bit block cipher with key values in the range 32 to 448 is used for securing the image.

**Al-Haj., et al.in [5],** "Digital image security based on data hiding and cryptography", proposed a hybrid algorithm that applied cryptography and watermarking to provide security to the medical images being transfer. This algorithm makes use of bit planes where it combines two images each consisting of 8-bit planes in a single image consisting of 16-bit planes. The first image of the 8-bit plane is watermarked using the RDH histogram shift method a copy of this is save and on the other hand encryption is performed on it and further, it is watermarked using the RDH histogram shift method. The combining process of two images takes place that is watermarked images and encrypted watermarked image each having 8-bit planes. This algorithm can be applied effectively to medical images of different modalities like CT, MRI, Ultrasound, and X-RAY. Using this hybrid approach its embedding capacity is increased.

REFRENCES:

[1] Aparna, V. S., et al. "Implementation of AES Algorithm on Text And Image using MATLAB." *2019 3rd International Conference on Trends in Electronics and Informatics (ICOEI)*. IEEE, 2019.

[2] Lather, Yashpal, Megha Goyal, and Vivek Lather. "Review Paper on Steganography Techniques." *IJCSMC, Signal Processing* 4.1 (2015): 571-576.

[3] Benedict, Arnold Gabriel. "Improved file security system using multiple image steganography." *2019 International Conference on Data Science and Communication (IconDSC)*. IEEE, 2020.

[4] Karolin, M., T. Meyyappan, and S. M. Thamarai. "Encryption and decryption of color images using visual cryptography." *Int. J. Pure Appl. Math* 118 (2018): 277-281.

[5] Al-Haj, Ali, and Hiba Abdel-Nabi. "Digital image security based on data hiding and cryptography." *2017 3rd International conference on information management (ICIM)*. IEEE, 2017.

NAME : KURALLA SRAVYA SAI SREE,

ENROLLMENT NUMBER :20STUCHH010265.