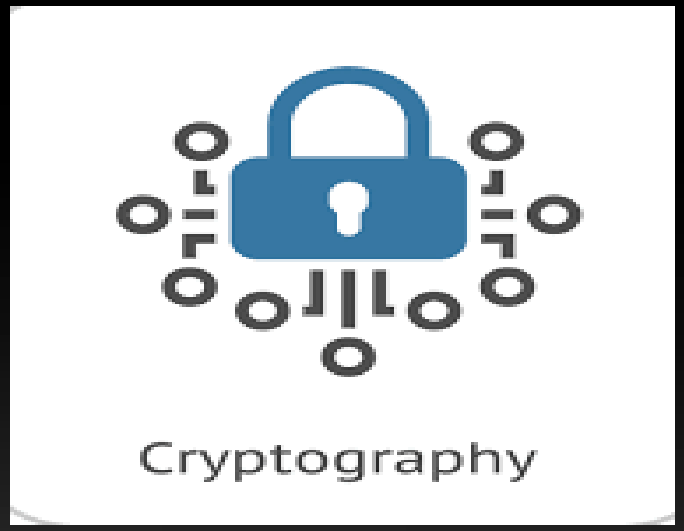
AES Image encryption and Decryption

Project presentation

Presented by:



6th semester 3rd year

CONTENTS

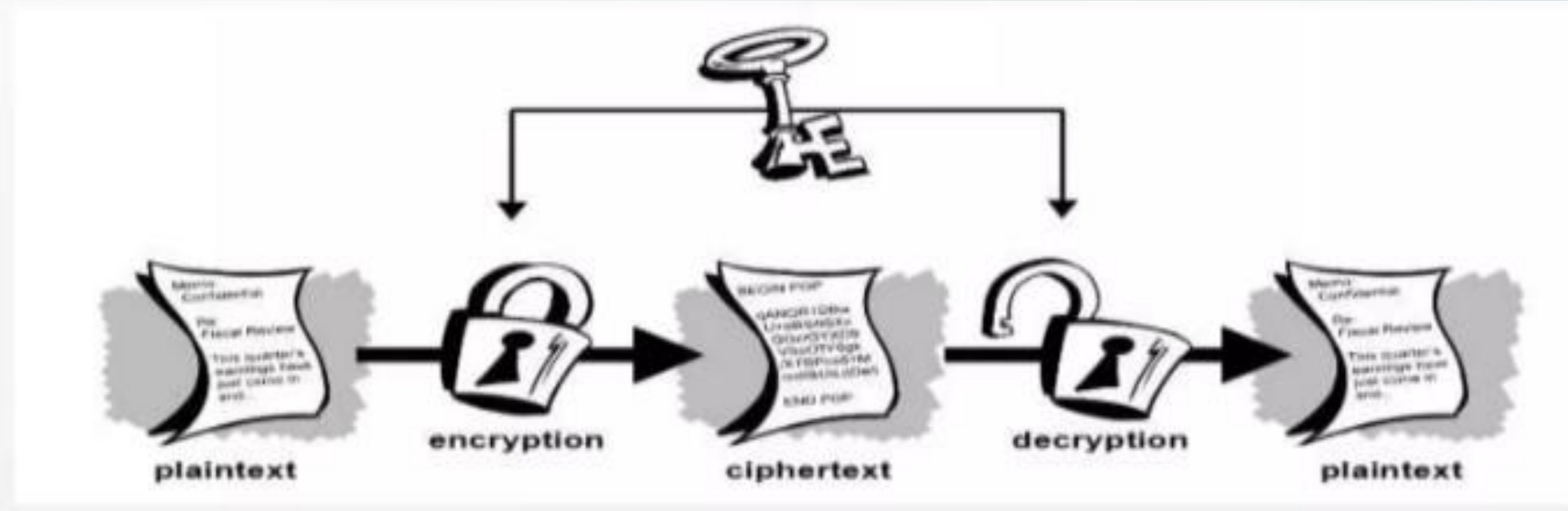
- BASICS OF CRYPTOGRAPHY
- AES ALGORITHM DIGRAMIC VIEW
- SHARES IMAGE ENCRYPTION AND DECRYPTION
- STEP BY STEP REPRESENTATION
- CONCLUSION
- REFERENCES

Basics of Cryptography

- AES encryption algorithm(Rijndael algorithm) is used .
- This algorithm uses 256 bit data block and may use three different key sizes128,196 and 256 bits.
- The 256 bits data block is divided into 16 bytes and are mapped into 4X4 array .
- Total number of rounds Nr is dependent on key length Nk.
- Main idea is that images can be viewed as arrangement of pixels ,bits and blocks

Cryptography KEY

Secret key Cryptography:



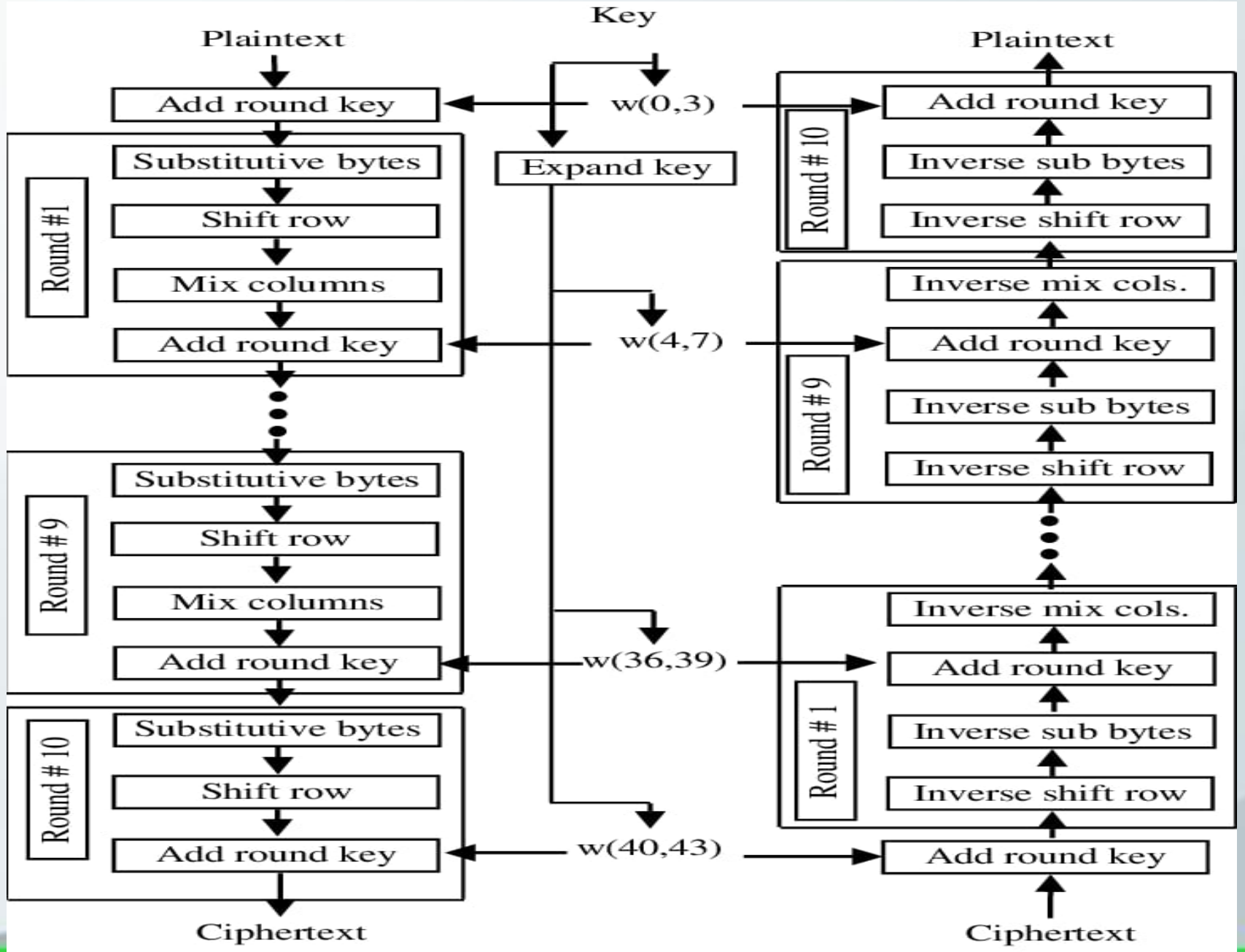
AES image encryption parameters

Algorithm	Key length, N_k	Block size, N_b	No of Rounds, $N_r=N_k+6$
AES-128	4	4	10
AES-192	6	4	12
AES-256	8	4	14

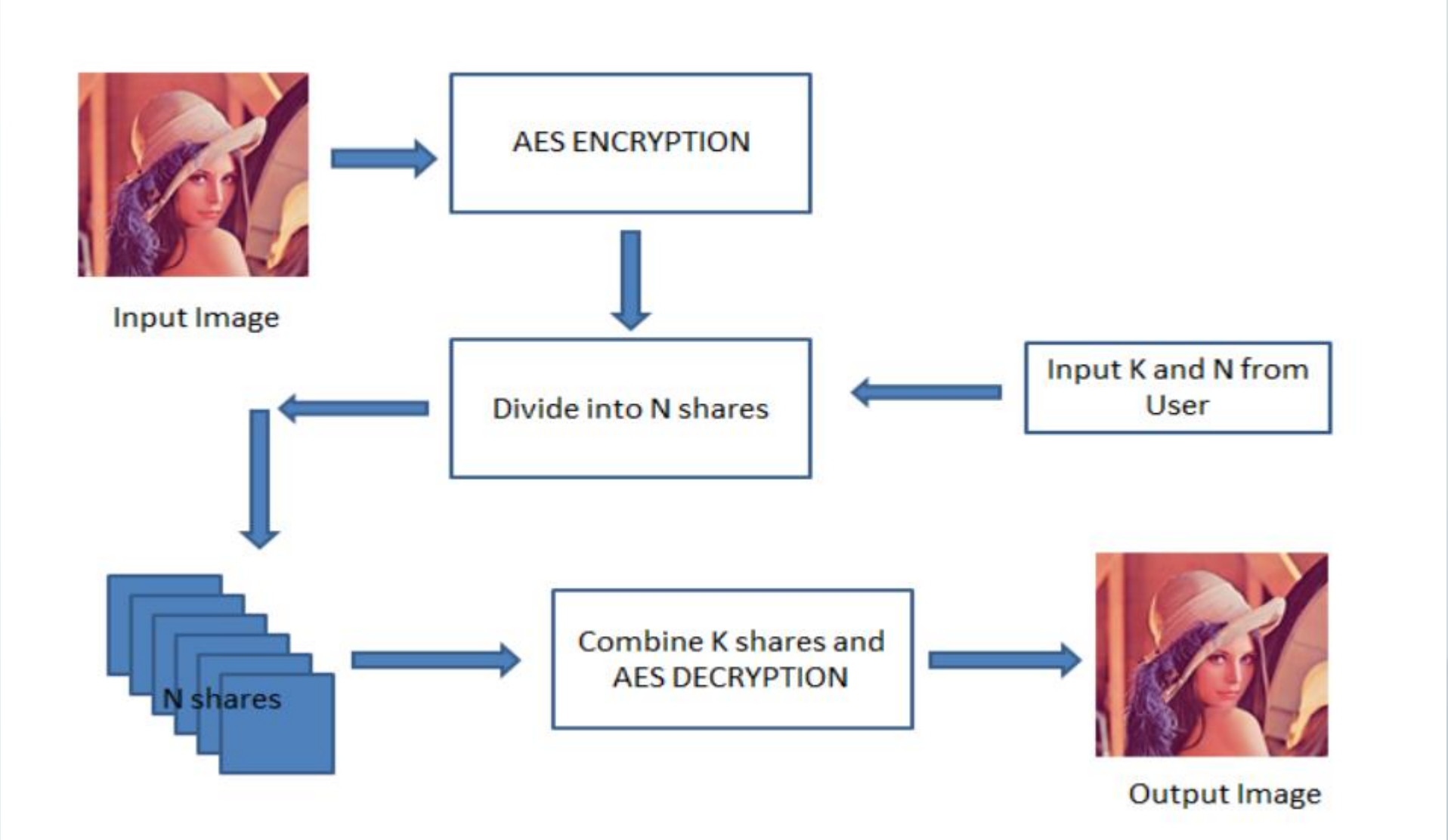
- AES operates on the : Binary finite field, GF(2^8).
- Each byte will be represented as a polynomial of at most degree 7:

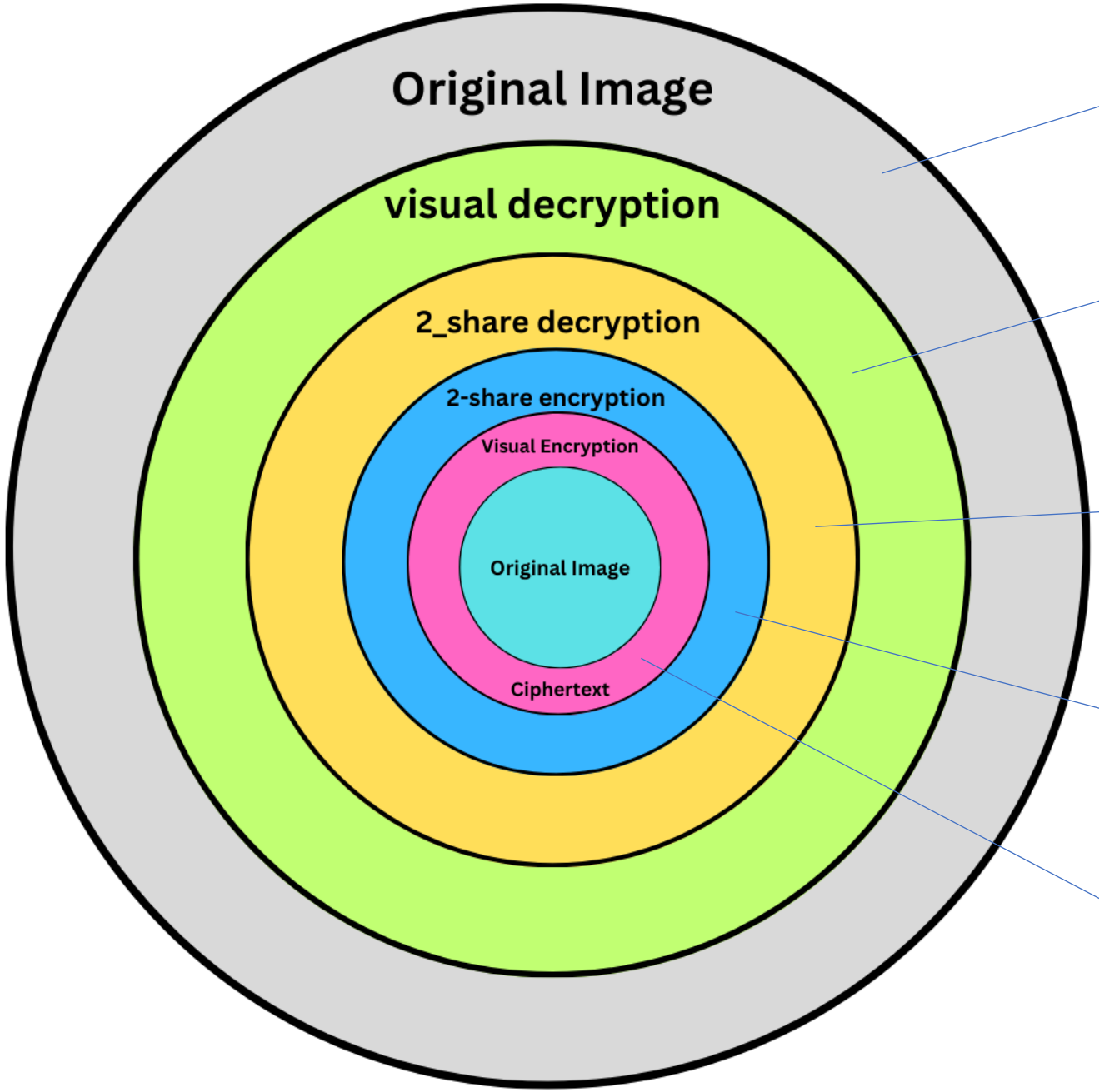
$$b_7X^7 + b_6X^6 + b_5X^5 + b_4X^4 + b_3X^3 + b_2X^2 + b_1X^1 + b_o$$

AES Algorithm



Shares Image encryption and decryption





Original Image

Conversion of ciphertext into Plaintext (AES image encryption)

Decryption using substitution ciphered image And secret image

Combination of secret and original image Using RGB random colors Convert into ciphered image

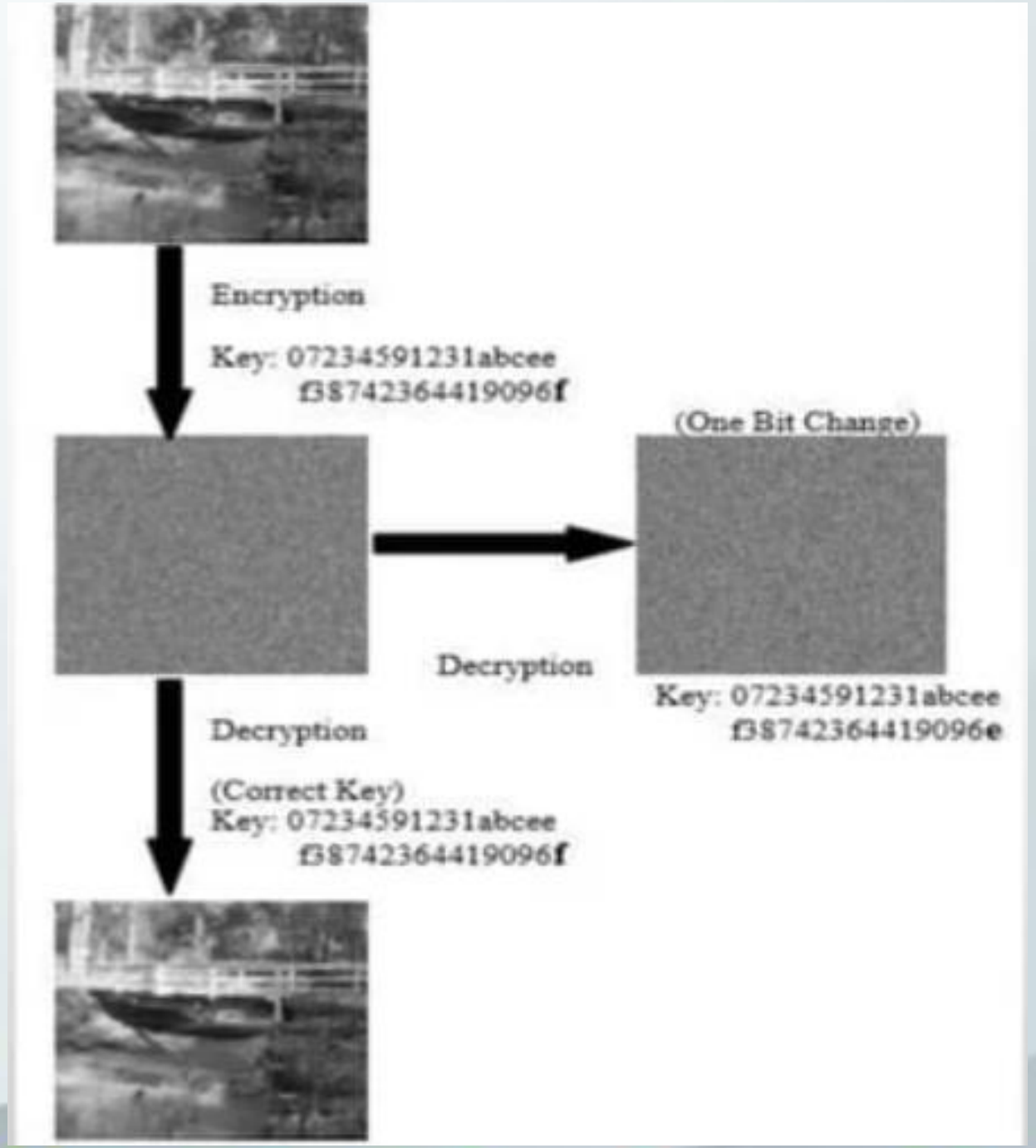
Conversion of plaintext into ciphertext (AES image decryption)

Steps followed for encryption and decryption

Ex:- bird.jpeg

Step 1:- bird.jpeg original image
Step 2:- [bird.jpg.crypt] containing encrypted ciphertext
Explain:- encrypt function used to convert plaintext into a ciphertext image
Step 3:- [visual_encrypt.jpeg] created for visual encryption
Explain:- conversion of ciphertext into visual image for creating encrypted image which then used for decryption

Step 4:- [secret.jpeg] containing RGB random colors.
Explain:- Random RGB color image it is seed or key in encryption
Step 5:- [2-share_encrypt.jpeg]
Explain:- created from combination of secret and ciphered image
Step 6:- [2-share_decrypt.jpeg] using generate back function
Explain:- decrypted image using generate back image
Step 7:- bird.jpeg original image


Encryption
Key: 07234591231abcee
f87423644190961
(One Bit Change)
Decryption
Key: 07234591231abcee
f87423644190961e
Decryption
(Correct Key)
Key: 07234591231abcee
f87423644190961

CONCLUSION

- The proposed algorithm offers high encryption quality with minimum computational time.
- The key sensitivity and key space of the algorithm is very high which makes it resistant towards brute force attack and statistical cryptanalysis.
- The time taken for encryption is relatively less in comparison with the algorithm proposed in the literature.

REFERENCES

1. Douglas Stinson, "Cryptography Theory and Practice", 2nd Edition, Chapman & Hall/CRC.
2. B. A. Forouzan, "Cryptography & Network Security", McGraw Hill Publication.
3. William Stallings, "Cryptography and Network Security", Pearson Education.
4. Dr. B. B. Meshram, TCP/IP & Network Security, SPD Publication.
5. Wenbo Mao, "Modern Cryptography, Theory & Practice", Pearson Education.
6. Hoffstein, Pipher, Silvermman, "An Introduction to Mathematical Cryptography", Springer.
7. Alang.Konheim, Computer Security and Cryptography, Wiley Publication.
8. A. Joux, "Algorithmic Crypt-analysis", CRC Press.
9. S. G. Telang, "Number Theory", McGraw Hill.
10. Matt Bishop, "Computer Security", Pearson Education.