I. INTRODUCTION

Visual Cryptography is a technique in which the image (visual secret) is decomposed into various shares which is distributed to different participants. Each participant knows that image, but stacking fewer than k shares reveals not any information about the secret image. Shares are usually presented in transparencies. Each participant holds a transparency (share). Unlike conventional cryptographic methods, VC needs no complicated computation for recovering the secret. The act of decryption is to stack shares and view the image that appears on the stacked shares simply. A (k,n) visual cryptography scheme is a visual secret sharing scheme such that stacking any k or more shares reveals the secret image, but stacking fewer than k shares reveals not any information about the secret image. In (2,2) visual cryptography each black and white pixels are divided into sub pixels hence after sacking the two shares, black pixel will remain black but the white pixel will become gray.

Digital watermarking is a technique which is used to identify ownership of the digital data such that image or video or document. Digital watermark is generally used for the copyright purpose. In digital watermarking, copyright icon or image is embedded into the cover image in such a way that the data of the image will not change in noticeable amount. There are two type of watermarking scheme. One is symmetric watermarking and the other is asymmetric watermarking. Most of the watermarking schemes are symmetric. In symmetric watermarking, the key which is used to embed and extract the data is same. Assume that we have an image named as A need to embed the watermark. With the help of the key X, watermark signal X can be stacked to host image A by some operation, the superposition is called open signal S and the process can be expressed as P = A ⊕ X where, ⊕ is an operation performed by special printing machine. In asymmetric watermarking scheme embed and extract key are different. For the embedding purpose the private key is used but when we want to extract, public key is used.

Some researchers have proposed an asymmetric digital watermarking scheme based on visual cryptography. In which the watermarked information is divided into two parts X = X_1 + X_2. One part is used to embed the watermark and the other part is used at the time of extraction. On the receiver side when we get the image then we extract the X_1 and then put X_2 and verify the image. If the image we got is X then we can assure that the image is not attacked.

II. PROPOSED ALGORITHM

Here we have two images. First image has the secret data or key which we want to distribute among the participant and the second image has the watermark (to authenticate the user). Here we divide the participants into two categories i.e. even participants and odd participants. Each participant knows that who are the even participants and who are the odd participants.

Step 1
Decompose the secret image A into n shares (A_1, A_2, A_3... A_n) by (n, n) visual cryptography scheme. Verifying image X is decomposed into 2 shares (X_1, X_2) by (2, 2) visual cryptography scheme.

Step 2
X_1 is embedded in all the odd number of shares of A i.e. A_1, A_3, A_5... and X_2 is embedded in all the even number of shares of A i.e. A_2, A_4, A_6... by asymmetric digital watermarking scheme. New shares are denoted by P_1, P_2, P_3... P_n.

Step 3
Now, odd numbers of shares are distributed to the odd participants and even numbers of shares are distributed to the even participants. Each participant will get only one share. All the participants know that how to extract the watermarked image from the given shares.

Step 4
All the odd participants extract the share \( (X_1) \) from their shares \( (P_1, P_3, P_5, ...) \) and all the even participants extract the share \( (X_2) \) from their shares \( (P_2, P_4, P_6, ...) \). Now, all the odd participant will stack their extracted share \( (X_1) \) on all the shares extracted by the even participants i.e. each participant of same category will stack their image on all the other participants of the different category one by one. If the watermarked image appears then these shares are not attacked in transmission.

Step 5
If the superimposition is not verifying image \( X \) then one of the two or both image have been attacked. To verify this, first we take the \( X_1 \) (from the faulty image) and \( X_2 \) (from the already verified image) and superimpose if we get the verifying image \( X \) then we can assure that \( X_1 \) is not attacked. Similarly we can check for \( X_2 \). If either of \( X_1 \) and \( X_2 \) can not reveal the verifying image then we identifies that owner is a cheater. When all the shares verifies then we superimpose all the shares \( (A_1, A_2, A_3, ..., A_n) \) and secret image will be recovered.

III. EXPERIMENTAL RESULTS

Here we have used (6,6) visual cryptography algorithm for secret and (2,2) visual cryptography algorithm for verifying image for experimental purpose.

Fig1. Secret Image A

\[ \text{NITIN} \]

Fig2. Verifying Image X

\[ \text{MNNIT} \]

Fig3. Odd Share A1

Fig4. Odd Share A3

Fig5. Odd Share A5

Fig6. Even Share A2

Fig7. Even Share A4

Fig8. Even Share A6

Here we have recovered the secret image and verified that all the participants are honest.

IV. SECURITY ANALYSIS

From the experimental results we can say that our scheme is as secure as the previous cryptographic scheme was i.e. no less than required number of participant can reveal the secret and if any participant will try to modify the secret image we can easily determine that and we are able to catch that cheater. But our scheme has a limitation. We need at least one
from the odd participants and one from the even participants to be honest. If all participants from both the side are cheaters then we are not able to know that which all (even or odd) participants are cheaters. We can also see that the watermarking of verifying image did not decrease the quality of the shares hence any person who see that shares with a naked eye is not able to determine whether there is a stego – information or not.

CONCLUSION

In today's rapidly growing internet world no communication is secured As we have seen in the previously proposed algorithm we need a secure way to transmit the second part of the verifying image to the participants. But in our proposed algorithm we don't need any secure channel. That is the major advantage over previous algorithm. Here we have to do only few computations because of the use of asymmetric digital watermarking algorithm. Rest all the encryption and decryption is based on human eye. Hence we do not need any other device. We can also improve the computation time by using hierarchical visual cryptographic algorithm instead of traditional visual cryptographic algorithm.

REFERENCES