ISSN 2186-5647

2-23

(2, 2)しきい値視覚復号型秘密分散法を用いたパスワード管理ツールの提案と評価

日大生産工(院)　○大川 直也　　日大生産工　栃窪 孝也

1　まえがき

視覚復号型秘密分散法とは，1979年にShamir[1]が提案した秘密分散法を画像に応用した手法であり，1994年にNaorとShamir[2]が提案している．この手法では，秘密にしたい画像を複数枚のシェアと呼ばれる画像に分散処理し，そのシェア画像単体からでは元の秘密の画像はわからないが，あらかじめ定められたしきい値以上のシェア画像を重ね合わせることにより，元の秘密の画像を復元することのできる秘密情報の分散管理方式である．

パスワードを利用した認証方式が世の中では主流となっており，一人のユーザーは複数のパスワードを管理することがほとんどであるが，複数のアカウントに同一のパスワードを設定してしまうことも少なくない．その人間の性質を利用し，セキュリティが脆弱なサイトをハッキングして不特定多数のIDとパスワードを入手することで別のサービスに対して不正アクセスを行うパスワードリスト攻撃が存在する．この攻撃に対応するために，近年では利用サービスごとに異なるIDとパスワードを設定することが推奨されている．

しかし，利用するサービスごとに異なるIDとパスワードを設定することは利用サービスの多い利用者からすると管理に労力を要する．一般的なところでも，免許証，クレジットカード，メールアドレス，Amazon，X(旧Twitter)，Netflix，楽天，Tポイントなどがあげられ一人で5つ以上のアカウントの管理を日常的に行なっている．

複数のパスワードを管理するツールも存在するが，そのツールにもマスターパスワードが必要となり，パスワードの管理は必要となる．

一方，2015年に視覚複合型秘密分散法を個人認証に適用する研究である覗き見を考慮した視覚復号型秘密分散法による個人認証方式を大岡と稲葉が提案している[3]．また，2017年にスマートフォンを用いた視覚復号型秘密分散法による個人認証方式を水野と稲葉が提案している[4]．大岡と稲葉の方式では，鍵となるシェア画像を1枚生成し，その鍵のシェア画像と0~9の数字を基にサーバーに保存するための各数字を秘密分散した10枚のシェア画像を生成している．この方式で作成されたシェア画像は鍵のシェア画像とのみ復元可能な(2, 2)しきい値になっている．鍵となるシェア画像を透明なシートに印刷し，サーバーに保存した10枚のシェア画像の中からランダムに選ばれた4桁のPINの1桁ごとと重ねることで認証に利用するPINを復元することができるという方式となっている．また，水野と稲葉の方式では，透明なシートではなくスマートフォンの利用へ変更することでより利便性を高めている．

そこで本研究では，パスワードの管理をセキュアにすることを目的とし，視覚復号型秘密分散法を用いたパスワードの管理を行うためのスマホアプリケーションとその評価を行う．本研究でも水野と稲葉の方式同様にスマートフォンを用いてシェア画像の復号を行うが，相違点は，シェアの生成方式である．本研究では，よりシェア画像の復号を行いやすいように秘密情報の文字サイズを下げて，ピクセルサイズを拡大する処理が行える．また，本研究では，PINのように特定のパスワードを対象とはせず，フリーなパスワードに対して視覚復号型秘密分散法を適用する．

2　準備

2.1　秘密分散法

Shamirの提案した(k, n) しきい値法とは，秘密情報をn 個のシェアに分割し，n 個のうち任意のk 個のシェアを集めることにより秘密情報を復元することができる手法であり，$k-1$ 個のシェアからは元の秘密情報がまったく得られない．

2.2　視覚復号型秘密分散法

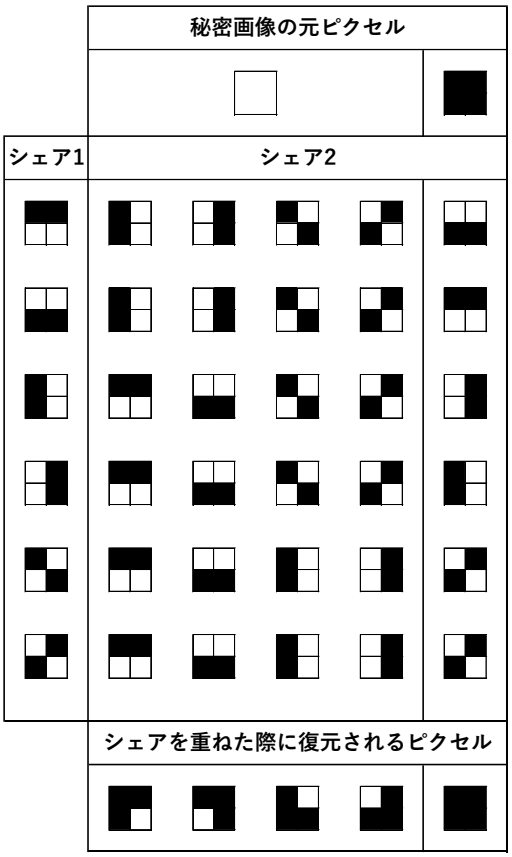
視覚復号型秘密分散法では，画像データに秘密分散法を適用する．一般的な(2, 2)しきい値型視覚復号型秘密分散法の場合，秘密画像データの1ピクセルを4分割し，シェア画像を

Proposal and evaluation for a password management tool using (2, 2) threshold Visual Secret Sharing

Naoya Ookawa and Kouya Tochikubo

重ねたときにOR演算により，秘密画像データの元ピクセルが黒であったら四つの黒ピクセルになり，白であったら三つの黒ピクセルと一つの白ピクセルになるようにシェア画像を定めて濃淡差を表現している(表1)．(2, 2)しきい値型視覚復号型秘密分散法の例を図1に示す．

表1　(2, 2)しきい値型視覚復号型秘密分散法のシェアの組み合わせ



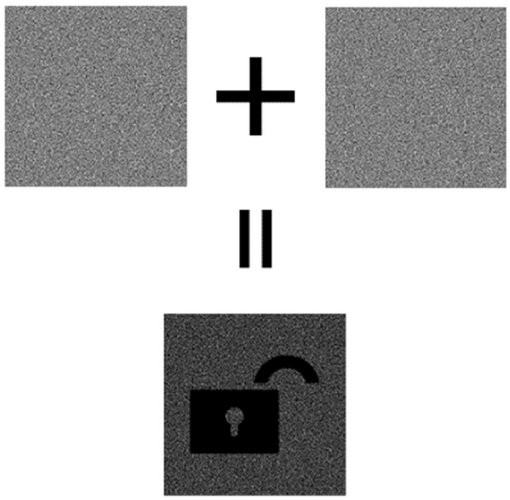


図1　(2, 2)しきい値型視覚復号型秘密分散法の例(左:シェア1，右:シェア2，下:復元画像)

3　パスワード管理ツール

3.1　画面構成

画面は3画面から構成されており，TOP画面，シェア画像生成画面，シェア画像表示画面となっている．

3.2　TOP画面

TOP画面(図2)は，シェア画像生成画面とシェア画像表示画面を繋ぐためのアプリケーション起動時の画面である．

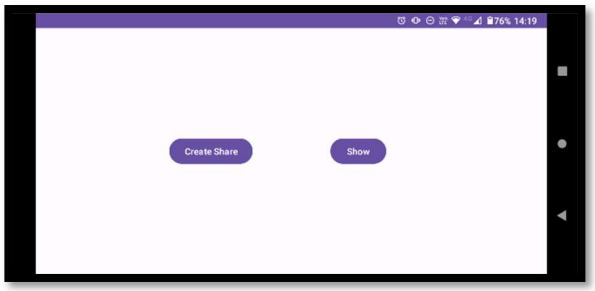


図2　TOP画面

3.3　シェア画像生成画面

シェア画像生成画面(図3)は，(2, 2)しきい値視覚復号型秘密分散法のピクセルパターンを用いてシェア画像を生成する．

図3　シェア画像生成画面

シェア画像を生成するにあたって以下の4つのパラメータを入力する．入力例を図4に示す．

① 画像名
作成するシェアの識別を容易にするために使用し，シェア画像それぞれの画像名と画像左上に表示する．

② 文字サイズ
シェア画像に埋め込むパスワードの文字サイズを設定するために使用し，利用者ごとに読み取りやすい(滑らかな)文字のサイズに調整することができる．

③ パスワード
シェア画像に埋め込む秘密情報に使用し，本研究では一般的なパスワードの長さとして使用されている8文字を最大文字数とする．

④ 倍率
作成したシェアデータのピクセル数を倍加するために使用し，この倍率を高めることでシェア画像の重ねやすさ(復号しやすさ)の向上を計る．

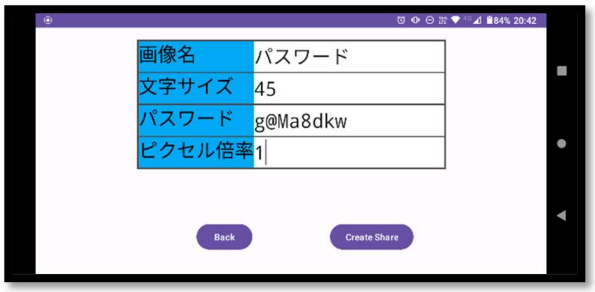


図4　パラメータ入力例

図5，6はアプリケーションで生成したシェア画像である．また，図7は2つのシェア画像を重ね合わせた復元画像である．

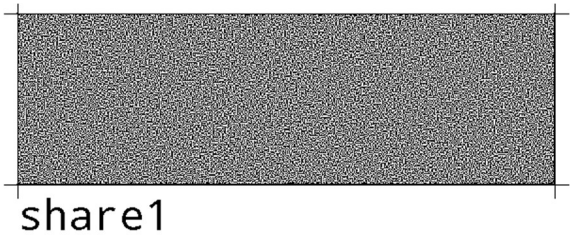


図5　シェア画像1(45px, 1倍)

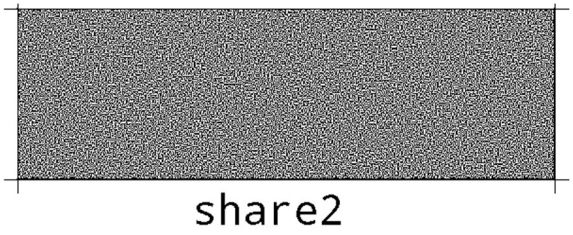


図6　シェア画像2(45px, 1倍)

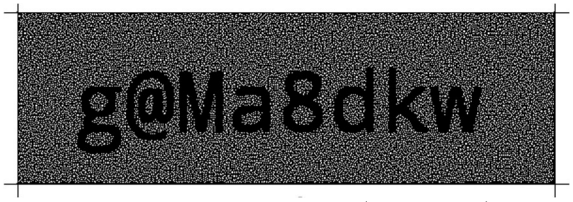


図7 理論値の復元画像(45px, 1倍)

3.4　シェア画像表示画面

シェア画像生成画面で作成したシェア画像を写真フォルダから選択して画面に表示する(図8，9)．スマートフォンの画面に表示したシェア画像と印刷したシェア画像(またはPC画面に表示したシェア画像)を重ね合わせることでパスワードの復号を行う．図10は，図5のシェア画像をスマートフォンの画面に表示し，図6のシェア画像を名刺サイズの紙に印刷し，復号を行った例である．

図10の復元画像を見てわかる通り，図5，6のシェア画像のピクセルサイズは小さいため，ピクセル同士を正確に重ね合わせての復号が困難である．

次に，同じパスワードで文字サイズを変更した場合の復元の変化について検証を行う．

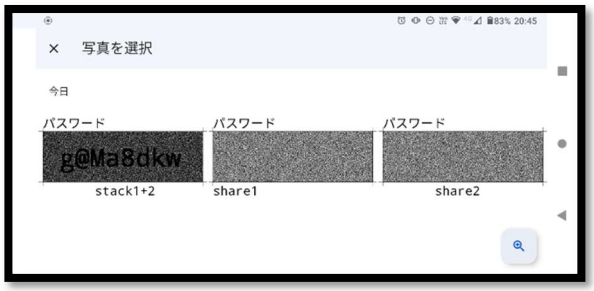


図8　シェア画像の選択

図 9　シェア画像表示画面

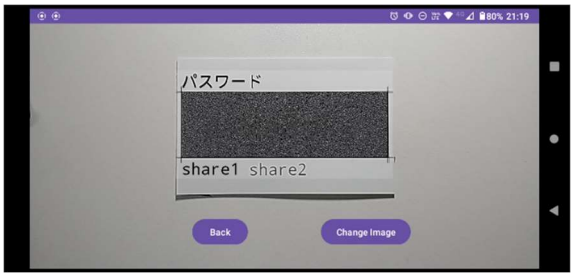


図10 ツールを使用した復元画像(45px, 1倍)

4　評価実験

作成したシェア画像とパスワードは同じで，文字サイズを3分の1の15pxにし，画面に表示する大きさを合わせるために倍率を3倍で作成した(図11, 12)．また，図13に2つのシェア画像を重ね合わせた復元画像，図14にスマートフォン上で復号した際の画面を示す．

図11　シェア画像1(15px, 3倍)

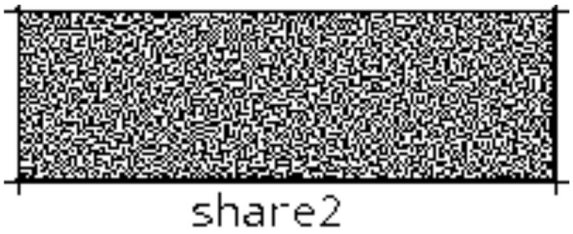


図12　シェア画像2(15px, 3倍)

図13　理論値の復元画像(15px, 3倍)

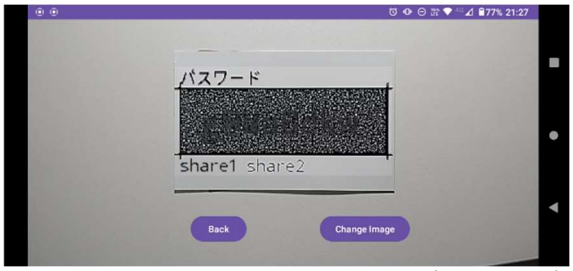


図14　ツールを使用した復元画像(15px, 3倍)

図14の結果から文字サイズを下げて，倍率を上げることで，復号する際のシェア画像を重ね合わせる際のズレの許容度が上がり，復元率の向上が見込めることが分かった．

ただし，今回の検証では文字サイズを15pxと45pxの2パターンでしか行えていないため，復号するにあたって最適な文字サイズや文字サイズごとの倍率については，より詳細な検証を行い全般的に示すことができるかは課題である．

また，性能面での今後の課題としては以下の3点があげられる．

① 単眼であるカメラの性質上シェア画像間の深度と角度を合わせることが難しいため位置合わせを行うための工夫が必要であること
② 今回，図14の画像を復号するにあたり，およそ1分30秒の時間を要したが，実利用を考慮した場合には，短時間での復号を行えるようにする必要があること
③ パスワードは仕事場(学校)と自宅の両方で使う可能性が高く，印刷したシェア画像を持ち歩くことは紛失するリスクがあるため，仕事場，自宅，スマートフォンのそれぞれにシェア画像を持てるように(2, 3)しきい値視覚復号型秘密分散法を本スマートフォンアプリケーションに適用すること

5　まとめ

本研究では，セキュアなパスワード管理を目的として視覚復号型秘密分散法を用いてシェア画像を生成し，スマートフォン画面上に表示したシェア画像と印刷したシェア画像を重ね合わせることで復号可能なスマートフォンアプリケーションのパスワード管理ツールを提案した．また，アプリケーションの評価を行い，本アプリケーションの想定通り文字サイズを下げて，シェア画像の倍率をあげることで復号を行う際の難易度は低減することを示した．

参考文献

[1] Adi Shamir, “How to share a secret”, Communications of the ACM, vol.22, no.11, pp.612-613, 1979.
[2] Moni Naor and Adi Shamir, “Visual Cryptography”, Lecture Notes in Computer Science vol.950, pp.1-12, 1995.
[3] 大岡 悠加, 稲葉 宏幸, “覗き見を考慮した視覚復号型秘密分散法による，個人認証方式の提案”, コンピュータセキュリティシンポジウム 2015, pp.1043-1049, Oct.2015.
[4] 水野 涼, 稲葉 宏幸, “スマートフォンを用いた視覚復号型秘密分散法による個人認証方式の提案”, ISEC2017-35, vol.117, no.125, pp.259-266, Jul.2017.