1C5-3

拡張された Arnold's CatMap のダイナミクスの検討

The study of the dynamics of the extended Arnold's CatMap

井上 聡[*1]
Satoru Inoue

[*1] 埼玉工業大学 工学部
Dept. of Engineering, Saitama Inst. Of Tech.

Previously, we proposed the CAPTCHA system using the dynamics of Arnold's CatMap. In this study we investigate the dynamics of extended Arnold's CatMap in order to clarify that it can be applied to our proposed system.

1. 序論

近年のインターネット接続利用者数はインフラの整備やその利用料金の低価格化，またネットワークサービスを利用するための，パソコン，タブレット，スマートフォンなど端末の普及がデジタルデバイスの高機能，低価格化にともない飛躍的に拡大している．またそれにあわせて，メールや SNS などの WEB サービスの種類も多様化しており，利用者にとっては非常に有用なサービスが拡充されていく一方で，それを利用するために必要なアカウントが bot と呼ばれるような自動実行エージェントによって大量に取得され，不正アクセスの一因となっていることもまた事実である．そのような不正を防止するために，いま WEB サービスにアクセスしているのが，正規に利用を目的としている人間であるのか，bot などの不正アクセスに関わる自動エージェントであるのかを判別する CAPTCHA (Completely Automated Public Turing test to tell Computers and Human Apart)と呼ばれる認証システムがある．基本的な CAPTCHA システムとは，文字列を読み取る能力で人間と機械とを判別する．システムは文字列に図や歪みを与えて加工したものを応答者に課題として提示し，その文字列を解読できたか否かで現在アクセスをしているのが人間なのか，それとも自動エージェントであるかを判別する．図 1.1 は一般的に利用される文字列読取型 CAPTCHA の一例である．しかしながら OCR などに代表される文字認識技術の向上により，既存の文字列読取型 CAPTCHA はエージェントにより比較的簡単に読み取られてしまうという脆弱性が指摘されている．それに対抗するかのように，文字読取課題が過剰なまでに難化し，本来は認証されるべき人間にすら判読が不可能となる，本末転倒な事態にもなっている．それらの問題を解決するように CAPTCHA システムはまた異なる方向性を持って変化をしていく．

図 1. Google で利用されている文字読取型 CAPTCHA の例

2. 先行研究

先述した問題点を解消するべく，CAPTCHA システムは文字読取型ものだけでなく，ユーザに 2 クラス分類問題を課す Assira と呼ばれるシステムや[Elson 2007]，文章の自然さを判断させる SS-CAPTCHA などが提案されている[山本 2009]．筆者らも従来の提案システムとはまた異なり，画像認識能力と文字列読取能力，また実装，運用の利便性を追求し，Arnold's CatMap と呼ばれるカオス写像を用いた CAPTCHA システムを提案している．本稿ではこの Arnold's CATMAP のダイナミクスを検討することを主たる目的としているが，その検討の契機を説明するためにまずは，筆者らが提案したモデルの核となっている Arnold's CatMap と先行した提案システムについて説明する．

2.1 Arnold's CatMap

Arnold's CatMap (CatMap)とは，パイこね変換と呼ばれるカオス現象の一つで，ロシアの数学者 Vladimir I. Arnold が猫の画像を用いたことからそう呼ばれるようになった[Arnold 1968]][Peterson 1997]．パイこね変換とは，パイ生地をこねるときの「伸ばす」，「折りたたむ」という工程を繰り返し行うことで生地内の含有物が最も効率よく混ざるということを数学的にモデル化したものである．CatMap における線形写像は次式(1)の通りである．

$$(x_{t+1}, y_{t+1}) = (x_t + y_t, x_t + \alpha y_t) \ mod \ N \qquad (1)$$

式(1)はある時刻 t において，座標(x_t,y_t)に存在したピクセルが次時刻でどの座標に移動するかを示している．一辺が N ピクセルの正方形の画像を横に α 倍，縦に α +1 倍に引き伸ばし，元となる画像サイズに切り取り，折りたたむことで画像の変換が行われる．図 2 上の様に CatMap による変換を行った画像は構成するピクセルの分布と画像サイズを保ったまま，オリジナルとは異なる画像に変換される．同様に変換後の画像にも再び CatMap の変換を行うと，画像はさらに細分化されオリジナルとは似ても似つかない画像へと変換される．繰り返し変換を行っていくにつれて画像はノイズのような状態に変化していくが，処理を一定回数繰り返し行うことにより，画像はオリジナルの状態に必ず復元される(図 2 下)．またその復元までの周期は正方画像の一辺 N に対して，線形ではなく非常に複雑な変化をすることが知られている．

連絡先：井上聡，埼玉工業大学工学部，埼玉県深谷市普済寺 1690，inoue@sit.ac.jp

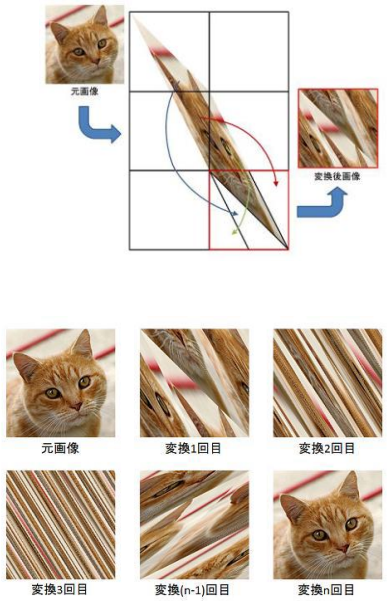

図 2. CatMap による画像変換 1 ステップ(上)と，繰り返しによる変換の様子(下)．

2.2 Arnold's CatMap を用いた CAPTCHA システムの提案

先行研究にて提案したシステムは CatMap により変換された画像を解答者がマウスクリック操作により復元し，画像中の文字列を答えることで画像の判別能力と文字の読取能力を問う CAPTCHA である．出題者(システム側)は単語をランダムに 3 種類選択し，正方形の画像に単語を配置して元画像を作成する(図 3 左)．元画像を CatMap の変換にかけ，変換画像を作成する．この時の変換回数は画像の判別が困難になるまで十分にランダムな回数(初期位相)行う．作成した変換画像を質問画像として解答者に提示する(図 3 右)．次に解答者は提示された質問画像をマウスの左ワンクリックにより画像に対して先述した式(1)が 1 回作用し，CatMap 変換が行われる．この操作を 3 種類の単語が可読になるまで繰り返し，元画像に書かれた文字列を読み取りキーボード入力により解答する．出題者は解答者の答えと選択された単語を確認し，一致している場合，解答者を人間であると判定する．図 3 に挙げた CAPTCHA システムでは一辺が 200 ピクセルの画像を用いている．この場合元画像に復元するまでの変換周期は 150 ステップである．すなわち質問画像は 150 から初期位相を減じたステップ数で元の画像に復元されることが保証されている．

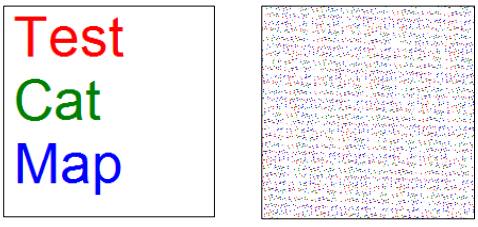

図 3. 初期画像(左)と CatMap 変換を任意ステップ施した質問画像(右)

2.3 先行提案システムの考察と問題提起

この提案システムを図 4 のような WEB ブラウザ上に表示される解答用インターフェースとともに構築し，画像提示・認証をする仮想実験を行った．

まずシステム運用性の観点から考察すると，ユーザに課題として提示される画像内に含まれる 3 つの単語は，システム内の辞書に登録したものから，ランダムに選択されて配置がされるような設計となっている．よって辞書に単語を登録するだけで，提示される画像のパターン数はほぼ無制限になるため，システムの運用はコストは非常に低くすることができ，また登録単語数を増やすことにより，システムの堅牢性を強固にすることが可能であるといえる．

また認証システムとしての観点から考察を行う．ユーザにコンピュータシステムへの操作と，画像の認識，文字を判読するという要素を内包する提示課題に対して，被験者の正答率は 98%という結果が得られた．また誤答例の 2%は“文字が判読できない”というものに起因するものではなく，単純なタイプミスによるものであり，従来の CAPTCHA システムで問題とされていたような，限りなく判読が不可能な文字により起きた誤答ではないことから，提案システムは既存システムの問題点をクリアしているといえる．

一方で，この提案システムは認証システムとして脆弱になり得る要素が含まれているのも事実である．その 1 つとして，今回のシステムでは提示される正方画像のピクセル数，すなわち式(1)の N が 200 で固定されている．CatMap 変換により画像が元の画像に復元される周期は式(1)の α (オリジナルの Arnold's CatMap では 2) と N の値によって一意的に決定されるため，これがシステムの脆弱性となる可能性がある．それを解消するには提示課題ごとに N を可変とすれば解決するが，この N の値によっては元画像への復元までのステップ数が数千となるものが存在する．すなわちそのような値を設定した認証課題は解答までにユーザに数千回のマウスクリックを要求することを意味し，そのようなパラメータを設定がされることは，現実的とはいい難い．

本稿は筆者らによる先行研究で認識された問題点をふまえたうえで，提案システムに適切なパラメータを設定するために，Arnold's CatMap による変換ダイナミクスを検討する．またあわせてさらなる提案システムの堅牢性を確保するために，オリジナルの Arnold's CatMap の式(1)を拡張し，α =2 以外の値を採用した際の写像の挙動を考察し，提案したシステムへの採用の可否を検討することを目的としている．

3. 結果

3.1 Arnold's CatMap(α=2)における変換収束ステップ数

Arnold's CatMap(式(1) α=2)において，画像が変換され m 元の画像に戻るまでのステップ数(以降、変換収束ステップ数と記述)は N の値によって一意的に決定される．N(=1~399)を横軸と変換収束ステップ数を縦軸としてその関係をプロットしたものを図 4 に示す．

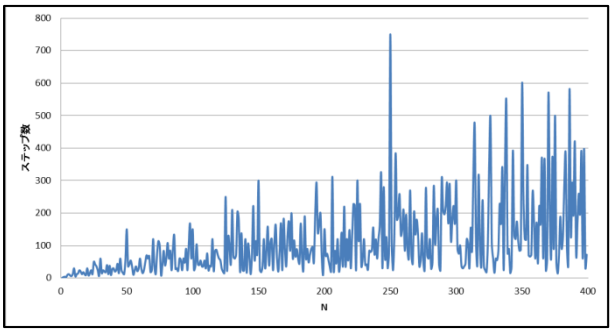

図 4.Arnold's CatMap の変換収束ステップ数の変化

これによると，α=2 における変換はすべての N において，必ず収束することが確認され，変換収束ステップ数は大域的には N の増加にともない増加する傾向にあるが，局所的には複雑な振動をしていることがわかる．このような複雑さが提案した認証システムの秘匿性に寄与することが考えられる．

3.2 拡張 Arnold's CatMap(α=2 以外)における変換収束ステップ数

ここで，式(1)のαをα>2 の値にして同様の計算を行った．まずはα=3 における，N(=1~399)を横軸と変換収束ステップ数を縦軸(片対数軸)としてその関係をプロットしたものが図 5 である．

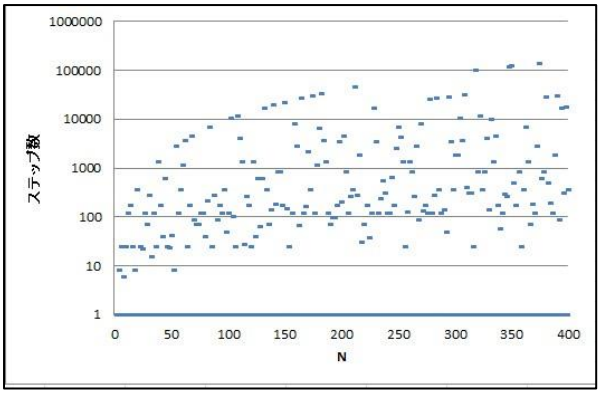

図 5.拡張 Arnold's CatMap(α=3)の変換収束ステップ数の変化

α=3 に拡張された Arnold's CatMap がオリジナルのものと異なる挙動として挙げられるのは，変換収束ステップ数が同一の N 値に対して大きく上昇しているものが多数観測されることである．またくわえて変換が収束しない N 値が多数存在することも確認されている．図 5 においてステップ数を 1 としてプロットしたものは，今回の計算において変換ステップ数 200000 回を上限として，その間に変換が収束しない，すなわち元の画像に復元されなかったことを便宜的に示している．α=3 において，変換が収束した N 値の個数は N=1~399 までの 399 通りのうちおおよそ半数の 200 通りであった．

ここでα=2~50 に対して，N=1~399 の中で変換が収束した N 値の個数を示したものが図 6 である．

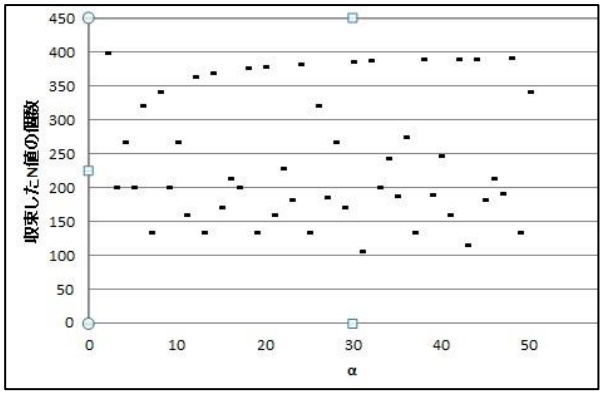

図 6. α=2~50 に対して変換が収束した N 値の個数

図 6 より，αと変換が収束する N 値に規則性が予見されたため，その内訳を観察した(図 7)．

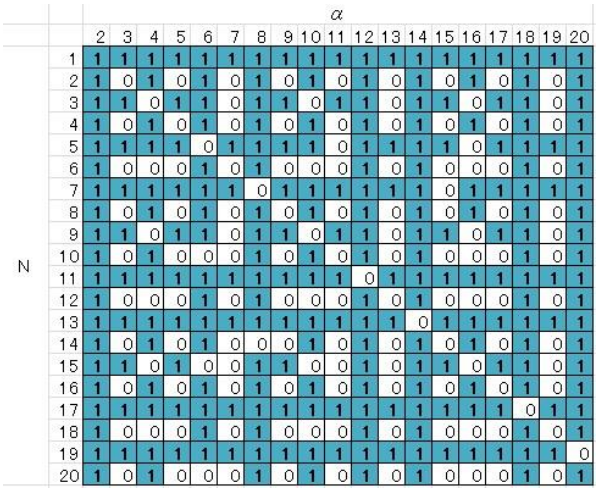

図 7. 変換が収束するαと N の組み合わせ

図 7 は横軸をα，縦軸 N として式(1)に適用した場合，変換が収束するα-N の組み合わせを 1，収束しない組み合わせを 0 として表示したものである．これによると N をとある値として収束するα の値を観察すると，ある種の周期性が確認できる．N=2,4 のときは収束するα値が 1 つおきに，また N=6 のときは“0,0,0,1,0”と収束の有無が周期的に出現している．これらを考慮して，変換が収束するα-N の組み合わせについて仮説を立てて推定を行った．

3.3 拡張 Arnold's CatMap(α=2 以外)におけるα-N の関係についての仮説

拡張された Arnold's CatMap において，あるαと N の組み合わせによる変換が収束するか否かを判定する方法を図 7 の結果より以下のように推定した．

＜判定の仮説＞

①αを素因数分解して，その素因数の集合を{P_i}とする．
αが素数の場合 $P_i=\alpha$.

②Nを集合{P_i}の要素で除した余りの集合を{R_i}とする．

③集合{R_i}の中に 1 つでも 1 が含まれていない場合，αと N の組み合わせによる CatMap の変換は収束し，1 が含まれている場合は収束しない．

という仮説に帰着した．なおこの仮説はこれまでに計算を行ったα=(3~100)，N=(1~399)までのすべての組み合わせで成立することを確認した．

4. まとめと今後の展開

4.1 結論

本稿では，拡張した Arnold's CatMap の写像式を検討し，筆者らが提案した CAPTCHA システムへの適用の可否について考察した．特に式(1)のαが 2 以外の場合，提案システムには非常に重要となる，画像変換の周期的再現性がないαと N の組み合わせが存在することが問題となるが，その再現性は 3.3 での述べた仮説により,判定する方法が確立できているため，特定のαと N の組み合わせを採用することが可能である．すなわち,変換が収束しないαと N の組み合わせ除外することにより,画像再現性が担保されることを意味し,提案した CAPTCHA システムへの適用は十分可能であるといえる．

4.2 今後の展開

(1) 仮説の立証

3.2 で論じた判定方法について，これまでの計算結果を適用した範囲で，その仮説に誤りは存在しないことが確認されているが，あくまで有限の解空間での議論である．この仮説を数学的に証明することにより，この判定方法やそれを適用した，提案 CAPTCHA システムの有用性や汎用性を主張できるようその方法を模索している．

(2) 変換写像ダイナミクスの検討

今回のダイナミクスの検討は，提案している CAPTCHA システムに適用可能なαと N を探索するという，2 次元パラメータ空間内での考察にとどまっている．提案した CAPTCHA システムは複雑なダイナミクスをもった画像変換を利用しているため，数値解析的な攻撃だけでなく，画像解析的な攻撃にも堅牢でなければならない．よって現在筆者らはある特定のα，N において，変換画像がどのような時系列変化をするのか，画像を構成するピクセルの遷移の様子をリアプノフ指数を計算して検討を行っている(図 8)．

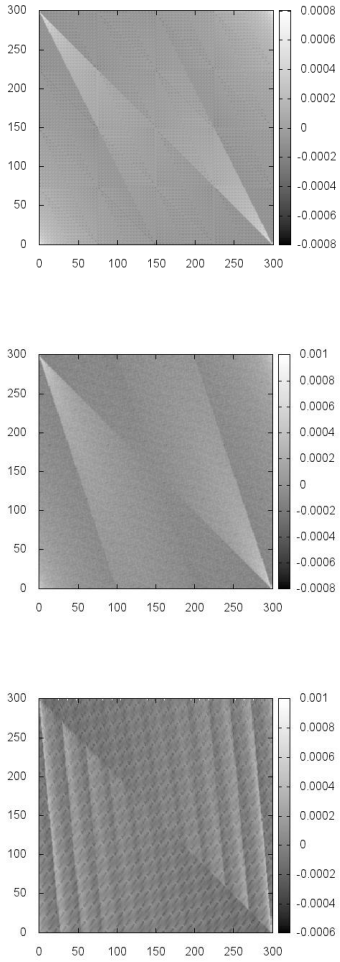

図 8. N=300　α=2(上)，α=3(中)，α=11(下)で画像変換した際の各ピクセル遷移の様子を表すリアプノフ指数

参考文献

[Arnold 1968] V.I.Arnold, A.Avez, "Ergodic Problems in Classical Mechanics. New York: Benjamin, 1968.

[Peterson 1997] Gabriel Peterson: Arnold's cat map. Math45-Linear algebra http://online. redwoods. cc. ca. us/instruct/darnold/maw/c atmap. htm, 1997.

[Elson 2007] J.Elson, J.Douceur, J.Howell, J.Saul: Asirra; a CAPTCHA that exploit interest-aligned manual image categorization, 2007 ACM CSS, pp.535-542, 2007.

[山本 2009] 山本 匠, 西垣 正勝, J.D.Tygar: 機械翻訳の違和感を用いた CAPTCHA の提案，情報処理学会研究報告．CSEC, [コンピュータセキュリティ]. 2009(37), p. 1-8, 2009.

[井上 2014]井上聡，Arnold's CATMAP のダイナミクスを用いた CAPTCHA システムの開発,第 28 回人工知能学会全国大会講演要旨集,1J3-1, 2014.